September 12, 2021

Eddy Kayihura Esq.,
Chief Executive Officer
AFRINIC Ltd.

Sir,

We refer to your letter dated 27 August, 2021 and your additional letter dated 10 September, 2021 Our response in reply to both of your letters are set out herein.

We find your letters to be entirely baseless and built on assumptions which are unproven and baseless and as yet unverified. Nonetheless, as contractually required, we are providing you with this fully informative response to the questions you posed in what can only be termed as defamatory and accusatory letters built on dubious information presented as proven facts.

Unless otherwise noted, references are to the text of your 27 August, 2021 letter (hereinafter referred to as "first letter"). Where we refer to your 10 September, 2021 letter, it will be so noted.

We take note of your references in paragraph 1 of your 10 September letter (hereinafter referred to as "second letter").

In your second letter, your paragraph 2 notes that you appear to have expected a response from us despite the fact that the deadline you chose has not yet lapsed. Despite the fact that AFRINIC has a history of taking months to respond to our correspondence, yet demands responses within a brief delay. To compound this you feign being offended that we have not responded even though your own choice of deadline for said response has not lapsed.

Be that as it may, we are addressing your response within the very short imparted deadline so as not to cause further aggravation. .

Regarding paragraph 3 of your second letter, we believe you have mis-stated the request. The request (to which you assented) was for ALL EXISTING INFORMATION AND EVIDENCE to support the claims and allegations of Mr. Hare-Brown in his affidavit

on 9 August, 2021. As such, we will take your subsequent paragraph 4 in the same letter to mean that no such evidence exists and that despite your due diligence with Mr. Hare-Brown to attempt to obtain such evidence, none was forthcoming. As such, we form the view that in all logic, Mr. Hare-Brown's affidavit is of no value and cannot be relied upon. To use Mr. Hare-Brown's allegations as if they are proven facts without having any verifiable supporting details is non-sensical to say the least. As they stand, his claims can neither be proven nor effectively disputed because they lack sufficient specificity. They are in the nature of innuendos and devoid of any substance.

Your statement at 1(a) is inaccurate as the undertaking you gave on behalf of AFRINIC does not in any way make our reinstatement temporary. While this was true of the original court order, the undertaking is not worded identically to the order and differs in this regard. Unless you intend to violate that undertaking, we consider this paragraph to be an inaccurate statement.

We note that in regards to 1(b) you are also in receipt of our response demanding actionable and/or verifiable details of this supposed abuse allegedly found by Mr. Hare-Brown. As already alluded to above, the content of his affidavit is totally unsubstantiated and an independent search by multiple experts has turned up no similar evidence.

We note that your paragraphs 1(c) and 1(d) are merely referential in nature and we acknowledge the existence of the documents in question, including our demand for supporting evidence to justify the baseless accusations and allegations in Mr. Hare-Brown's affidavit and your inexplicable refusal to provide same; instead you are resorting to baseless and unfounded accusations.

With regard to your paragraph 2, the content of Mr. Hare-Brown's affidavit cannot possibly be considered evidence as it merely contains unproven allegations and does not offer sufficient actionable details as to verify or falsify or even properly investigate his claims. As you have noted, there are more than 6 million addresses issued to Cloud Innovation. We are aware of at least 1,500,000 web sites hosted within those 6 million addresses. As such, Mr. Hare-Brown's numbers are highly suspect from the word go. We have sampled a much larger number of web sites within our address ranges and have found no instances of content that would be considered illegal in the jurisdictions where the content is hosted, no instances of illegal streaming of copyrighted content,

and absolutely no instances of indecent images of children. AFRINIC and Mr. Hare-Brown have refused to provide actionable or verifiable information and are thus deemed unable to substantiate the allegations. Any action by AFRINIC based on these spurious allegations will be met with the full force of actions, locally and internationally and at all levels, by Cloud Innovation

Therefore, regarding paragraph 5 of your second letter, regardless of any expertise Mr. Hare-Brown may or may not have, your inability to produce actual verifiable evidence means that his affidavit and your belief in it is very revealing of your state of mind. As such, we do not find it compelling and will not expend further resources on this wild goose chase. Mr. Hare-Brown must be compelled to provide supporting verifiable evidence or in the alternative his affidavit must be stricken from the record as an invalid set of baseless assertions rather than evidence.

Regarding the allegations at paragraph 6 of your second letter, we note the following:

1. All of the extant technologies for dealing with data at rest require the data to be locally available on a machine running the search software. Since we do not host customer content on our hardware and do not have any form of network shares from our customer's systems, these technologies are not viable in our environment.

2. All of the extant technologies for dealing with data in motion require the ability to tap the network at a point that the data traverses. Since we are not inline in the data path of our customers or their customers, there is no viable way for us to effectively implement such a tap.

3. It might be possible to implement a keyword searching web-crawler, but the legality of doing so in many jurisdictions is questionable at best.

4. We are not aware of any ISP who has, as yet, implemented such technologies at scale, nor are we aware of any web hosting services which engage in such regular monitoring of their customer's systems. In short, AFRINIC is attempting to imply that extraordinary monitoring which is not performed by virtually anyone in the industry and which requires the use of very expensive cutting-edge technologies is commonplace and normal among ISPs, Content Hosting providers, etc. It most certainly is not. Generally, these technologies are so expensive as to be applied by governments and law enforcement agencies who then provide actionable abuse

complaints to the service providers in question, as we have repeatedly requested from both AFRINIC and Mr. Hare-Brown.

5. None of Mr. Hare-Brown's statements lead us to believe that he found content on our systems. Indeed, it could be possible that he found the content on systems owned and operated by our customer's customers (or potentially even more levels distant from us) and not our systems.

6. We refute your claim that responsible ISPs utilise such technologies on a regular basis as we have seen no evidence to support the claim and our queries to several responsible ISPs in multiple countries inquiring as to what technologies they use for this purpose have been answered with "nothing, we depend on abuse reports mostly from law enforcement."

We take note of the quote of section 4(b) and 4(c) of the RSA and clause 5.5.1.14 of the CPM in your paragraph 3. We accept that these are accurate copies of the content of those sections.

Regarding your paragraph 4, while the issues raised are serious, the way in which they have been raised affords us no opportunity to verify, let alone address them and is a clear case of AFRINIC acting in completely bad faith without regard for solving the issues, but rather in an effort to use these allegations as an excuse to take an action previously prohibited by the courts and already enjoined by virtue of the undertaking signed by you. As such, we reject the entire premise on which all of the subparagraphs for your paragraph 4 are built, but we will, nonetheless, refute each and every one of them individually below.

While there is no evidence as yet suggesting that we have committed any illegal acts, instead of seeking such evidence, AFRINIC has chosen to ask us to prove that we are taking steps to stop engaging in illegal activity. We cannot stop that which we have not started. And Since AFRINIC is a private enterprise, we did not see how AFRINIC could act as law enforcement to start such investigation on a third party, and how such self-proclaimed law enforcement act would have any relation to our contractual obligations.

Paragraph 4.1(a) assumes that we host the sites in question and that it has been proven that:

A. We host the sites in question

B. That the sites in question have illegal, unlawful, dangerous, and/or amoral content

Neither of these allegations is yet proven and you have offered no evidence to support the allegations beyond the fact that Mr. Hare-Brown was willing to sign off these baseless and unverifiable allegations. Since, as stated in his affidavit, these allegations cannot be verified as he does not provide sufficient detail to validate or investigate his claims, this cannot possibly meet any rational standard for evidence and therefore his affidavit is merely a signed allegation and nothing more.

We do not host the number of web sites claimed by Mr. Hare Brown. We do provide addresses to other providers, some of whom host web sites and some of whom provide addresses and connectivity to others who host web sites. Many of those web sites contain user generated content. Further, Mr. Hare-Brown's claims about how some of our addresses are routed were true more than 2 years ago, but are not true today, again making his information suspect to say the least.

Paragraph 4.1(b) again assumes that we host the sites in question as above and further assumes that:

A. We allow the sites to contain the content alleged

B. We have some form of duty to monitor the content of the sites in question

C. We have done an inadequate job in the performance of this alleged duty.

Each of these assumptions is false. We do not host the web sites, but rather they are likely on infrastructure numbered with our addresses by our customers. We not only have no duty to monitor the content of web sites managed by our customers and their customers, but it is illegal for us to do so in many jurisdictions. No web hosting provider engages in such monitoring and the current industry standard is to respond to abuse complaints (at least actionable ones) as they are received. While we acknowledge that AFRINIC and Mr. Hare-Brown have provided something that sort of looks like a complaint (albeit through a rather odd channel), they have not only neglected, but refused to provide sufficient details and information as to make said complaint

actionable (or even verifiable). Though we are not a web hosting company, I believe that this shows not only do we lack such an obligation as assumed in 4.1(b) of your letter, but our customers don't have such an obligation either. It is appalling to see an RIR offering up such allegations which reflect such a complete misunderstanding of the industry best practices and technical feasibility. We are of the view that this can only be explained by the apparent bad faith on the part of AFRINIC in their relentless efforts to find an excuse to destroy our business by any means necessary.

Paragraph 4.1(C) of your letter assumes that:

A. The sites in question are allowed to engage in these activities

B. The activities alleged are illegal in the jurisdictions where the sites are hosted

C. That so-called amoral content has some level of independent universal definition which can be enforced

D. That so-called amoral content being present on our IP addresses violates our RSA

E. That we are the network police or that AFRINIC has determined itself to be the network police and expects us to act as its deputy and that this obligation is enshrined somewhere in the RSA or the AFRINIC governing documents.

Each and every one of these assumptions is also false. We do not allow sites to engage in illegal or unlawful activities. Depending on how you intend to define dangerous (there are those that would argue a site which advocates peaceful protest against certain government actions is dangerous and AFRINIC itself has made arguments that sites supporting Cloud Innovation's side of this very suit are a danger to the entire RIR system), we're not sure of the basis for that being prohibited by the RSA. If you mean sites advocating violence or terrorism, those are not allowed under our contracts.

Further, it's not clear (since we haven't been able to obtain sufficient information due to AFRINIC's obstreperousness) what jurisdictions the sites named are in (if they even exist) or whether the content alleged is actually unlawful or illegal in those particular jurisdictions.

We think the failure of assumptions C, D, and E is self-evident.

Paragraph 4.1(d) fails because it depends entirely on the incorrect and invalid assumptions above.

The state of affairs has, as near as we can tell, been brought about by a consultant hired by AFRINIC making unfounded and baseless allegations in an affidavit while failing to provide any form of evidence to support the allegations and refusing to offer sufficient details so as to make it possible to investigate, validate, verify, or even identify the alleged violations. We think the state of affairs was further compounded by AFRINIC assuming that such a baseless and poorly formed set of assertions could be considered evidence by any competent definition of the term and then asserting a number of invalid assumptions built on this house of cards.

As such, we would very much appreciate it if AFRINIC would withdraw these claims and allegations or provide actionable and credible evidence to support them. In the event actionable evidence is provided, the sites will be investigated and appropriately addressed as we do with any actionable abuse complaint provided. For clarity, this does not mean that we accept AFRINIC's judgment of what constitutes unlawful or illegal, nor does it mean that we accept any obligation to inflict some arbitrary "moral" code upon our customers or their customers. If a site contains truly illegal or unlawful content, we will have it taken down and/or terminate the customer, if necessary. If the site merely contains content that AFRINIC dislikes which is legal in the jurisdiction where it is hosted, then there is little we can do within the law to act against a customer who is not actually breaking the law. While we realize that AFRINIC clearly believes that it is perfectly valid to attempt to enforce upon its members some form of rules and restrictions which are not supported by law or contained in its governing documents, we prefer to abide by what the law says.

Your paragraph 4.2 is built on the assumption that we are required to put measures, means, and/or processes in place to prevent such things. We have an obligation to act on legitimate and actionable abuse complaints and we do just that. It is our considered opinion that our obligations in such matters are adequately addressed in doing so. It is further built on the assumption that the sites numbered within our address space are "our sites". This is as wrong and false to claim as it would be to claim that the sites numbered within (e.g. Seacom's) address space are AFRINIC's sites.

Your paragraph 4.3 is inappropriate and disproportionate to our contractual obligations. Unless AFRINIC can show a legitimate need for a list of all sites hosted by us in order to perform its obligations under the RSA, this is an unnecessary demand for privileged customer data and goes well beyond any reasonable performance required by the RSA. If AFRINIC is able to get a ruling from a court of competent jurisdiction that providing such information is required under the RSA, we will happily provide it. Until such time, we believe that the request violates the spirit of the RSA and also likely violates various privacy laws of Mauritius and other nations where our customers operate. Since we believe the request to be unlawful, we believe we have no obligation under the RSA to comply with it.

Your paragraph 4.4 is answered in the affirmative. Our standard customer contracts have been submitted in previous filings with the Mauritius court and have therefore been served upon AFRINIC. We, therefore, refer you to those filings for the remainder of your answer. But for good measure we do so again. To show our good faith, an extract of our standard contract is being enclosed at the end of this letter.

The five composite questions in your paragraph 4.5 are answered in sequence as follows: no, yes, see A below, see B below, and see C below.

A. The dates would be numerous and the research necessary to retrieve them within the deadline provided would be impractical. The request is out of line and the information requested would provide no probative value to any investigation related to the AFRINIC RSA. If AFRINIC can return with an order from a court of competent jurisdiction finding that they are entitled to the information under the RSA, we will happily provide it, but for now, we believe the request to be unsupported by law or the existing contracts between AFRINIC and Cloud Innovation.

B. Some sites were found not to be violating our policies. Some sites were found to be in violation and were taken down by our customers or their customers. Some customers were terminated for abuse.

C. Your request asks for the disclosure of privileged communication(s) between Cloud Innovation and its attorneys, privileged attorney work product, and privileged communications between Cloud Innovation and its customers. As

> such, your request is rejected on the grounds that we believe it is unlawful and is not supported by the RSA. If AFRINIC can obtain an order from a court of competent jurisdiction claiming that their request is, in fact, supported by the RSA and it would be legal for us to comply, then we will of course, comply with such an order.

The three composite questions in your paragraph 4.6 are answered in sequence as follows: yes, See C above, and See B above.

Your paragraph 5 is answered as follows: Please clarify any and all circumstances under which additional information would be required and the nature of those requirements. Please make sure to justify any and all future requests for information by tying each and every specific request to a specific provision of the RSA, CPM, or AFRINIC bylaws which actually and specifically justifies the request. Please verify that such requests are lawful and that complying with them would not be illegal or unlawful on the part of Cloud Innovation. While AFRINIC and its staff may have nothing better to do, we are attempting to run a business here and the overhead of addressing AFRINIC's repeated and insistent requests for information in its continuing pursuit of destroying our business have become abusive.

As to your paragraph 7, we would expect nothing less. Nonetheless, we believe that evidence and facts will show that we have done nothing illegal and have not committed any crimes. As such, your useless threat causes us no fear. However, rest assured that should AFRINIC decide to execute this threat on the back of these spurious allegations, Cloud Innovation will take every and all available actions, locally and internationally, to vindicate its rights both against AFRINIC and any such of its officers who wield the power inside AFRINIC to destroy Cloud Innovation.

Finally, as to your paragraph 7 of your second letter, we will note that the only valid contractual obligation contained in either letter is the requirement that we respond to you. There is no requirement that we respond in the manner or format that you demand, nor is it reasonable for you to place a time limit on our response that is less than the average time it has taken us to get a response from AFRINIC (which we compute at approximately 6 months to date). As such, this letter not only denying your claims but rebutting your innuendos is quite sufficient to meet our contractual obligations.

Cloud Innovation

Innovate Cloud

Regarding paragraph 8 of your second letter, stand advised that we also reserve all of our rights under our contract with AFRINIC and under the undertaking of Mr. Eddy Kayihura on behalf of AFRINIC not to terminate our membership.

Further, we believe that the obligation not to terminate extends to an obligation to preserve the status quo and renew our membership next January so long as we pay our invoice(s) as expected. As such, this letter should serve as notice to AFRINIC that we intend to pursue all of our rights to preserve our utilization of the addresses and abide by the terms of the contract as they are written.

We do not accept any additional obligations which AFRINIC continues to attempt to imply that are not written in the contract and we will continue to demand AFRINIC's performance under the contract and the undertaking.

Sincerely,

Paul Lam

On Behalf of Cloud Innovation

Extract of Standard Contract

(2) Customer will not use the IP addresses for any illegal or abusive purposes including SPAM, SPAM email marketing and will otherwise comply with Service Provider's **Acceptable Use Policy** as set out in **Schedule B**.

(3) In the event that Service Provider receives any complaint regarding usage of the IP addresses, Service Provider will immediately notify Customer and Customer will take immediate action to investigate and remedy any such complaint. The Customer will be charged of service fee $20 USD / IP / incident, which shall be settled within 7 days from the date of invoice issued by the Service Provider. Overdue payment will lead to suspension of the IP addresses without any further notice provided by the Service Provider.

(4) In the case that the total sum of abuse service fee exceeds 50% of the yearly fee of the IP delegation service under this agreement, the Customer shall provide Service Provider with the written reason, or any other form of methods to convey the Customer's reason as may be instructed or permitted otherwise by the Service Provider, of the occurrence of the corresponding abuse activities as well as a plan to remedy such situation. If no favorable and constructive answer is provided by the Customer within fourteen (14) days from the date of the Customer's total sum of abuse service fee exceeds 50% of the yearly fee of the Service, the Service Provider reserves the right to suspend the IP addresses without providing any or further notice to the Customer. Any damage or loss suffered by the Customer due to the afore-mentioned suspension should be at the Customer's cost and expense and, for the avoidance of doubt, the Service Provider shall not be liable for the Customer's loss and/or damages suffered due to the aforementioned suspension. The Customer shall pay the Service Provider an administrative cost of $1,000USD each time for the suspension, which shall be paid in full before the resumption of the IP addresses. No compensation of time will be given for loss of service time due to the suspension taken by the Service Provider.

(5) Failure to remedy any violations of the Acceptable Use Policy within 48 hours will result in immediate loss of usage of those IP addresses without the Service Provider being liable to the Customer. Customer will also be responsible for any out of pocket costs associated with improper use of IP addresses and costs to repair any harm or damages caused by this improper usage. In the case of the Customer violation of the Policy of RIR (Regional Internet Registry) or this Agreement, the Service Provider has the right to suspend the service with no any refund.

SCHEDULE B
ACCEPTABLE USE POLICY

Customer agrees they (and its employees, agents or others with access through Customer to the IP space) have to follow the policy of RIR (Regional Internet Registry) and will not:

(a) Use the IP space for any unlawful purpose, including without limitation (i) intentionally or knowingly transmitting, receiving, or disseminating any obscene, pornographic, threatening, defamatory or other unlawful information or information which infringes upon legal rights of others, including intellectual property rights, (ii) intentionally or knowingly accessing accounts, servers, websites, data, hardware or software not intended to be accessed by Customer; or (iii) engaging in any kind of fraudulent transaction or conduct.

(b) Intentionally or knowingly use the IP space to transmit, receive or disseminate any information or material which could be expected to offend a reasonable person due to indecent, harassing, racially or ethnically discriminatory, violent or otherwise offensive content.

(c) Use the IP space to transmit or disseminate unsolicited bulk messages, including advertisements, informational distributions and charitable or other solicitations. Customer agrees to pay for all cost, expenses and fee damages that may occur associated to any black list removal as a result of usage by Customer or Customer's users.

Customer has to take immediate actions regarding child pornography and terrorism complaints. The abuse contact must ALWAYS be available 24 hours x 7 days a week.

In case of disputes, the Service Provider reserves the right to make the final decision.