Publication of Memorandum of information I Continuous phishing and Phishing incident response

Nr.	Continuous phishing, Phishing incident response or General question	Subject	Document	Question	Answer
1	Phishing Incident response	Scope	Request for Proposal, section 1.1 (Description of the Assignment)	Can Enexis clarify whether the contractor is expected to be responsible for the full handling of phishing incidents (including mitigation and closure), or whether responsibility for follow-up and resolution remains with Enexis?	The substantive handling (human analysis, selection and execution of mitigating actions) is carried out by the Enexis IT SOC. The Contractor provides the PIR tool that offers the workflow and supports this work in the manner described.
2	Continuous phishing	Scope	Schedule of Functional Requirements, section 3 + 4	To what extent does Enexis expect the contractor to actively manage and optimize phishing campaigns and awareness programs, versus providing tooling and support for internal teams?	Please refer to Appendix 02.1 - paragraph 4.2 Campaign Management.
3	General question	Scope	Schedule of Functional Requirements, section 2.2	Can Enexis clarify the expected level of integration with Microsoft solutions (such as Sentinel, Defender, and ServiceNow), and whether the contractor is responsible for configuration and ongoing management of these integrations?	Depending on the architecture and technical setup proposed by the Contractor, the optimal division of management responsibilities between the supplier and Enexis will need to be determined. We consider it likely that the decision will be that the cut-over point of responsibility for ongoing management lies at the integration's receiving end in our target system, while the Contractor will take the lead in the initial technical implementation of the end-to-end process, and that the Contractor will closely monitor any announced changes in dependent applications/components that affect the process' outcome and, if necessary, will adjust the design accordingly.
4	General question	Scope	Request for Proposal (general PIR scope)	Can Enexis specify the expected response times and service levels for phishing incident response?	We do not expect human first line incident response or triage to be performed by the Contractor. Please refer to our answer to question 1. For service levels regarding product support and technical performance requirements, please refer to the non-functional requirements in Appendix 02.2.
5	General question	Scope	Schedule of Functional Requirements, section 1.1.2	Can Enexis clarify whether end-user communication and training within the service must be provided in Dutch, or whether this can be flexibly determined depending on the target audience?	Default language must be in correct Dutch. The End user can decide to change the language to at least English. Please also refer to requirement 1.1.2 in Appendix 02.1.
6	General question	Q&A	N/A	As the first Q&A round is currently open, we would like to clarify the process for the subsequent round. As we joined the project at a late stage, we were not able to involve all relevant internal stakeholders in time to consolidate all clarification points for submission. Could you please confirm whether tender participants will be allowed to submit new questions in the second Q&A round (i.e., questions not raised in Round 1)?	It is possible to ask new questions in the second Memorandum of Information. The deadline for the second Memorandum of Information is monday 11 May 2026, before 10:00 AM.
7	General question	Award criteria	Part III (Method used and score)	You indicate that for each sub-award criterion (SC 1.1 and SC 1.2) a maximum number of three A4 pages applies. Request to please accept at least six A4 pages per SC. In addition, could you please confirm that the cover page/front page and the table of contents are explicitly excluded from the A4 page limit/page count?	Enexis will not comply with your request. Enexis sees no reason to increase the maximum number of permitted pages per Sub-award Criterion, given what Enexis ask from Tenderers for each Sub-award Criterion. For this reason, Enexis asks Tenderers to adhere to the maximum number of permitted pages as stipulated in the Request for Proposal. Enexis confirms that the cover page/front page and the table of contents are explicitly excluded from the A4 page limit/page count.
8			Request for Proposal – Continuous phishing and Phishing incident response: Section: 2.3 Minimum Requirements and Eligibility Requirements (ER) >> Technical competence, general ER 4	Enexis is asking for a SaaS solution, as such we would strongly recommend ISO/IEC 27701 and ISO/IEC 27017 + 27018 certificates as well. Should tenderers comply to these standards as well?	No, the Tenderer must have an information security management system that meets the requirements of ISO 27001 (or equivalent). If the Tenderer does not possess an information security certification, the Tenderer must have an information security policy/manual. See for more information paragraph 2.3 in the Request for Proposal. Tenderers may, by means of security certification, additionally to the requirement ER4, substantiate how they guarantee that the proposed solution functions properly and remains secure in sub-award criterion 1.2. It is up to the Tenderers to demonstrate how they guarantee that the tool will continue to function properly and remain secure (sub-question 2, sub-award criterion 1.2).
9	Phishing Incident response		Appendix 2.2 non-functional requirements: SOC workload & volumes	'What is currently the percentage false positives vs real threats?	Ignoring these numbers to contain a minor amount of duplicates, in a recent period of 90 days 238 incidents (containing one or more similar email submissions) were escalated to IT SOC, of which 85 were closed with determination Malicous.
10	Phishing Incident response		Appendix 2.1 functional requirements. Section 2: Phishing incident response (PIR)	Could Enexis clarify the preferred balance between automated triage and manual SOC validation for reported phishing emails?	Ideally, the PIR tool would every time be successful in automatically reconstructing the full campaign and execute all required mitigation actions with the same outcome as that of a SOC analyst. The extent to which the Contractor's tool cannot be relied upon to do this determines the need for additional human analysis and handling, and that extent therefore depends on the proposed solution. Mind that, in line with the current overall phishing threat landscape, we currently have a relatively low risk appetite in this regard.
11	Phishing Incident response		Appendix 2.2 non-functional requirements: SOC workload & volumes	'What is the average and peak volume of reported emails per month today?	The monthly number of individual phishing email reports between October'25 up to March'26 ranged between 760 and 3,535, with an average of 1,307. Mind that the currently used PIR tool groups similar reported emails together into one incident and only incidents matching escalation criteria are followed up by Enexis IT SOC. This ranged between 59 and 112 incidents, with an average of 89.
12			Appendix 2.1 and 2.2 functional and non functional requirements: Compliancy to the requirements	How can tenderer provide overview of compliancy on all functional and non-functional requirements? Or will Enexis assume full compliancy by default when submitting a response.	By submitting a Proposal, the Tenderer confirms full compliance with all stated functional and non-functional requirements. An overview of compliance may be requested as part of the evaluation process. Compliance will be further verified during the verification meeting scheduled for 15 July 2026, where the intended solution and its alignment with the requirements will be discussed and validated in more detail. Enexis reserves the right to verify compliance throughout the entire contract period.
13		Data protection		Can you clarify your requirements regarding data residency and jurisdiction for security tooling, particularly for phishing incident response data (e.g., email content, headers, user metadata)?	The Tenderer shall provide a solution in which all data is stored, processed, and managed exclusively within the EEA. Please refer to Appendix 02.2 requirement 19.
14		Data protection		How does Enexis assess the acceptability of solutions that may be subject to non-EU legislation (such as the US CLOUD Act), even when all data is stored and processed within the EU?	The Tenderer shall provide a solution in which all data is stored, processed, and managed exclusively within the EEA. Please refer to Appendix 02.2 requirement 19.
15		Reporting		Referring to Functional Requirement 3.1.4. Is it acceptable that detailed phishing incident data remains restricted to administrative roles, while end users are provided with summarized or contextual feedback through the platform?	End users are allowed to review the data they submitted themselves. Information produced through processing of the submission should be limited to what generally would be of added value to the End user, like, for example, the state, classification/determination category, detected threat type and a (closure) note specifically intended for the End user to read. Any other data should be exclusively available to roles generally requiring it for their objective.
16		Operational model		The scope of the RFP is Continuous phishing simulation tool and a Phishing incident response tool. Questions CP4.2.4. til CP4.2.8 are focused on the capabilities and support of the Contractor. Please explain the desired operational model and roles/responsibilities of Enexis and the Contractor.	Enexis defines policy, KPIs and scope, is owner of the objectives and provides governance and oversight. The Contractor operates the Continuous phishing service end-to-end, maintains the platform, and provides proactive advice, reporting, trends and improvements.

Nr.	Continuous phishing, Phishing incident response or General question	Subject	Document	Question	Answer
17		Reporting		In the document Functional Requirements under requirement 3.1.2, 3.1.5 and 4.2.10. is stated that the tool and reporting must include End User training performance. Are security awareness training programs for end users part of the requested scope?	The requested scope includes End user training performance reporting, but this should be interpreted specifically in relation to Continuous phishing. Security awareness training programs for End users, such as computer based training (e learning modules), are not part of the Assignment. However, Continuous phishing campaigns, including reporting on End user performance and simulation results (e.g. click rates, reporting rates, and trends over time), are explicitly in scope and required as part of the tool and reporting capabilities.
18		Implementation		What are the responsibilities of Enexis and the Contractor in the implementation plan in regards to who does what and in what extend the Contractor has access to the current tooling (Microsoft Defender&Sentinel, ServiceNow) at Enexis to integrate the Phishing Simulation and Phishing Incident Response tool.	Depending on the architecture and technical setup proposed by the Contractor, the optimal division of management responsibilities between the supplier, Enexis and any required third party consultancy will need to be determined. We consider it likely that the decision will be that Enexis will perform the hands-on changes within our existing applictions and platforms in close collaboration with engineers or the architect from the Contractor, without the Contractor requiring access themselves.
19		Implementation		What defines Enexis as an “effective implementation” in the implementation plan criteria?	An effective delivery is deemed to have taken place when the delivered outcome has been provided in full, demonstrably and in accordance with the predefined requirements, is functionally deployable within the organization, and has been formally accepted by Enexis. Please mind that "effective" is stated in the background information in sub-award criterion 1.1, providing context to what we hope to achieve with the actual requirements stated below it.
20		Availability & Disaster Recovery		"To what extent does Enexis expect the prime contractor to own: - Support (L1/L2/L3), related to non functional requirement 3a and 3b? - Incident response operations, related to non functional requirement 3a and 3b? - Platform configuration and administration, related to non functional requirement 4a and 4b?"	The Contractor is responsible for the availability and timely recovery of both tools, primarily for the components that fall within the Contractor’s scope. In addition, the contractor must proactively prevent announced changes by vendors to components within Enexis' scope from disrupting the process, for example by monitoring vendor roadmaps and release notes.
21	Phishing Incident response	Integrations		Is the Contractor expected to implement and maintain integrations with Microsoft Sentinel, Defender and ServiceNow, or only provide integration capabilities (APIs, connectors)?	Depending on the architecture and technical setup proposed by the Contractor, the optimal division of management responsibilities between the supplier and Enexis will need to be determined. We consider it likely that the decision will be that the cut-over point of responsibility for ongoing management lies at the integration's receiving end in our target system, while the Contractor will take the lead in the initial technical implementation of the end-to-end process, and that the contractor will closely monitor any announced changes in dependent applications/components that affect the process' outcome and, if necessary, will adjust the design accordingly.
22	Phishing Incident response	Definitions		Can Enexis confirm that ‘supporting the entire reporting process’ refers to providing tooling capabilities (workflow, automation, integrations), and that operational activities such as incident analysis, decision making and follow-up actions remain the responsibility of Enexis or its SOC?	Confirmed. To meet other functional requirements, for example regarding efficiency and limiting the operational workload of the Enexis IT SOC, the Contractor's tool can offer automating parts of the analysis and mitigation activities.
23		Periodic Contract Evaluation, Audit and Benchmark, Enexis Purchasing Conditions 2025		"In order to have auditing more balanced, is Enexis willing to modify Art. 11.2 to the following ? ""Enexis has the right to have an audit conducted once a year to verify the correct compliance with the agreement by the Other Party. The Other Party shall reasonably cooperate with such audit. Each party shall bear its own costs in connection with any audit. However, if the audit demonstrates a material non-compliance by the Other Party, the Other Party shall reimburse the reasonable and demonstrable external audit costs incurred by Enexis, provided that such costs are proportionate and pre-approved. In the event that a material non-compliance is identified, Enexis shall be entitled to conduct follow-up audits, provided that: •Such audits are limited to verifying remediation of the identified non-compliance, •No more than one additional audit per 12-month period may be conducted, and •Such right shall expire 12 months after the initial audit identifying the non-compliance"". "	Enexis does not agree with the proposed amendment. The suggested limitations and cost-sharing mechanisms would have a waterbed effect: reducing audit flexibility would require compensatory measures elsewhere in the agreement to manage compliance and regulatory risk. Given Enexis’ regulatory responsibilities, the current audit clause represents a necessary and balanced allocation of risk and will therefore not be amended.
24		Periodic Contract Evaluation, Audit and Benchmark, Enexis Purchasing Conditions 2025		Would Enexis be willing to include the following article?: The Other Party shall have the right to object an audit being performed by a third party that is a direct competitor of the Other Party".	Enexis agrees with your proposal, provided that it is substantiated that there is a direct competitor. Enexis has added article 5.1 sub b to the Agreement. Article 5.1 sub b: *Addition to Article 11 of the Enexis Purchasing Conditions 2025: The Other Party shall have the right to object an audit being performed by a third party that is a direct competitor of the Other Party, provided there are valid reasons to believe that it concerns a direct competitor of the Other Party.*
25		Periodic Contract Evaluation, Audit and Benchmark, Enexis Purchasing Conditions 2025		Would Enexis be willing to include the following article?: "Enexis will notify the Other Party in writing at least 14 days prior to an audit".	Enexis agrees with your proposal. Enexis has added article 5.1 sub c to the Agreement. Article 5.1 sub c: *Enexis will notify the Other Party in writing at least 14 days prior to an audit*

Nr.	Continuous phishing, Phishing incident response or General question	Subject	Document	Question	Answer
26		Termination, Enexis Purchasing Conditions 2025		"Art. 18.2 is unbalanced and unfavorable for the Supplier. Can Enexis agree to add this article: ""In the event that Enexis terminates the Agreement, in whole or in part, for convenience pursuant to Article 18.2, Enexis shall pay the Supplier a termination fee equal to: (a) all fees for Services performed and accepted up to the effective date of termination; (b) any non-cancellable commitments and third-party costs reasonably incurred by the Supplier in connection with the Agreement; and (c) an amount equal to the fees that would have been payable for the remaining term of the Agreement, up to a maximum of twelve (12) months of fees, as compensation for early termination. The termination fee is intended to compensate the Supplier for investments made, committed resources, and loss of anticipated revenue, and shall be payable within thirty (30) days of the effective termination date. The Supplier shall take reasonable steps to mitigate its costs following receipt of a termination notice""."""	Upon further consideration, Enexis has decided to withdrawal article 18.2 from the procurement terms and conditions. The revised procurement terms and conditions will be shared after completion of the publication of Memorandum of Information 1. The deviations from Appendix 08 are included in Article 4 of the Agreement (Appendix 03).
27		Liability, Enexis Purchasing Conditions 2025		"We believe that the current liability provisions place a disproportionately high level of risk on the Supplier, particularly in light of the nature of the services provided and the role as a reseller of third-party solutions. In line with standard market practice, we propose that liability is limited to 100% of the annual fees paid by Enexis to the Supplier under the Agreement. This ensures a fair and balanced allocation of risk that is proportionate to the commercial value of the contract. Furthermore, we propose that indirect and consequential damages (including loss of profit, revenue, or business opportunities) are expressly excluded, as is customary in comparable agreements. We believe this approach provides appropriate protection for both parties while maintaining a commercially reasonable risk profile. Can Enexis accept this?"	Enexis does not agree with your proposal.
28		Intellectual Property, Enexis Purchasing Conditions 2025		"The Candidate is of the opinion that the conditions for Intellectual Property are unbalanced. Can Enexis agree to the following? ""Each Party shall retain ownership of all Intellectual Property Rights, including Know-how and information, that it owned or developed independently prior to or outside the scope of the Agreement ("Background IP"). To the extent that any deliverables are specifically created for Enexis under the Agreement ("Foreground IP"), Enexis shall obtain a non-exclusive, perpetual, worldwide, royalty-free license to use such deliverables for its internal business purposes. Nothing in this Agreement shall result in a transfer of ownership of Intellectual Property Rights from the Supplier to Enexis, except where expressly agreed in writing. The Supplier retains all rights, title and interest in and to its underlying technology, methodologies, tools, software (including third-party software), and know-how used in the performance of the Agreement. Each Party agrees to cooperate, where reasonably required, to give effect to the rights and licenses set out in this Article""."""	In the Agreement (Appendix 03, article 5.1), Enexis has incorporated your proposal regarding intellectual property, with the addition that this article shall apply provided that the proprietary rights can continue to be exercised after termination of the Agreement. Article 5.1 a) *Addition to article 13 of the Enexis Purchasing Conditions 2025: Each Party shall retain ownership of all Intellectual Property Rights, including Know-how and information, that it owned or developed independently prior to or outside the scope of the Agreement ("Background IP"). To the extent that any deliverables are specifically created for Enexis under the Agreement ("Foreground IP"), Enexis shall obtain a non-exclusive, perpetual, worldwide, royalty-free license to use such deliverables for its internal business purposes. Nothing in this Agreement shall result in a transfer of ownership of Intellectual Property Rights from the Supplier to Enexis, except where expressly agreed in writing. The Supplier retains all rights, title and interest in and to its underlying technology, methodologies, tools, software (including third-party software), and know-how used in the performance of the Agreement. Each Party agrees to cooperate, where reasonably required, to give effect to the rights and licenses set out in this Article*
29	General question	Reference Statement	Appendix 12	Core Competence 1 requires a minimum of 1000 users. For the required and proven solution it is not relevant how many users are provided with the solution. Supplier request you to withdraw the minimum users in Core Competence 1.	Enexis does not comply with your request. This requirement is deliberately set to ensure that the solution has demonstrable scalability, stability, and performance in a real-life context. Given that Enexis will provide services to approximately 8,000 End users, the minimum threshold of 1,000 end users is considered both reasonable and proportionate. A solution proven with only a very limited number of users would not provide sufficient assurance that the solution can reliably support the required scale, complexity, and operational demands.
30	General question	Phishing	Request for Proposal	Can you confirm that the scope of the request is not limited solely to phishing simulation and phishing incident response via email, but also includes other channels? For example, via Teams or other communication channels?	Enexis confirms that the request is not limited solely to Continuous phishing and Phishing incident response in the context of email. Phishing via other communication channels is also permitted, in order to address related future threats.