DIGITAL SECURITY & PRIVACY ADDENDUM
(DV&P ADDENDUM)

between

[NAME OF COUNTERPARTY]

and

Enexis Netbeheer B.V.
Enexis Personeel B.V.[1]

dated [date]

1 Include the Enexis entity signing the Master Agreement.

Initials Enexis

Initials Counterparty

TABLE OF CONTENTS

Initials Enexis

Initials Counterparty

THE UNDERSIGNED:

1) [Enexis Netbeheer B.V.] a private limited liability company with its registered office in 's-Hertogenbosch, with its place of business at 5223 MB 's-Hertogenbosch at Magistratenlaan 116, registered in the trade register of the Chamber of Commerce under number 17131139, legally represented in this matter by [name] [designation] and [name] [designation], hereinafter referred to as: Enexis

1) [Enexis Personeel B.V.], a private limited liability company with its registered office in 's-Hertogenbosch, with its place of business at 5223 MB 's-Hertogenbosch at Magistratenlaan 116, registered in the Trade Register of the Chamber of Commerce under number 66934389, also acting on behalf of the other companies belonging to the group and legally represented in this matter by [name] [designation] and [name] [designation], hereinafter referred to as: Enexis

and

2) Counterparty [name and legal form] with its registered office at <registered office address>, having its place of business at <address>, registered in the Trade Register of the Chamber of Commerce under number [Chamber of Commerce number], legally represented in this matter by <name <designation>, hereinafter referred to as: the Counterparty;

Each individually referred to as a '**Party**', and collectively as the '**Parties**'.

Whereas:

- The parties have entered into the agreement [name of agreement] with an effective date of [date] (hereinafter: the **Master Agreement**), and the Enexis Purchasing Terms and Conditions 2025 (hereinafter: **T&Cs**) have been declared applicable to the Main Agreement. The Main Agreement relates to [description of goods, services and work];
- Due to its role in the vital infrastructure of the Netherlands, Enexis is considered an essential entity under the Cybersecurity Act (*Cyberbeveiligingswet*, **Cbw**) and a critical entity under the Critical Entities Resilience Act (*Wet weerbaarheid kritieke entiteiten*, **Wwke**). As such, it is bound by strict laws and regulations regarding security and continuity;
- Given the vital nature of Enexis' public duties in transporting electricity, gas and heat, any system failure, disruption or compromise could have serious consequences for quality of life and business operations in large parts of the Netherlands;
- Enexis is responsible for implementing and maintaining appropriate security measures with the Counterparty;
- Enexis continually evaluates and improves security measures between the parties in order to anticipate and respond to emerging threats and risks;
- Enexis has conducted a Digital Security & Privacy Impact Analysis (**DV&P Analysis**) regarding the goods, services and/or work covered by the Master Agreement and determined the risk to be "high";
- In this DV&P Addendum, in addition to the Master Agreement, the Parties record their agreements regarding the security measures to be implemented and maintained.

The following has been agreed:

Initials Enexis Initials Counterparty

DEFINITIONS

When this DV&P Addendum uses terms defined in the T&Cs, those terms will have the same meaning as in the T&Cs. The Parties will also use the following definitions in this DV&P Addendum:

Definition	Description
Access Security	it involves granting access to authorised persons or systems in a controlled manner, whereby access by unauthorised persons or systems is prevented by implementing technical measures.
Activities	Despite the T&Cs, this term refers to all activities to be performed by the Counterparty under the Master Agreement.
Confidential Information	Information that has been expressly described by Enexis as confidential, or that should reasonably be assumed to be confidential based on its nature and content. In any case, this information pertains to Enexis's security.
Critical Third Party	a third party that supplies goods or services, or performs activities, which are so essential that their unavailability could lead to the interruption or limitation of the distribution of heat, electricity or gas.
DV&P Analysis	it is an internal Enexis analysis that indicates the level of security risk for Enexis as "medium" or "high", based on, among other things, the nature, continuity risks, and the degree of access to Enexis information and locations by (employees of) the Counterparty.
Incident	as an exception to Article 32.17 of the T&Cs, an incident is defined as a security breach that threatens or (partially) compromises the availability, integrity or confidentiality of information, or an event that could adversely affect the continuity or quality of the processes, goods and/or services of the Counterparty and/or Enexis, including a Breach.
Information	data, information (including Personal Data), databases and information (including Confidential information) relating to Enexis' business operations in the broadest sense. This includes all information provided by or on behalf of Enexis, whether orally, in writing or otherwise, prior to or during the Master Agreement, as well as all documents and data in any form that contain, reflect or arise from information provided to the Counterparty in connection with the performance of the Master Agreement.
Least Privilege Principle	this is a security concept and operational measure whereby each user, process or system within an organisation or domain is granted only the access rights and permissions necessary to perform essential tasks and functions.
Security Measures	the entire set of policies, processes, procedures and technical measures that safeguard the availability, integrity, quality and confidentiality of all forms of information, processes, goods and/or services belonging to Enexis and the Counterparty, and that mitigate and remedy the consequences of incidents and/or breaches.
Personal Data	all information relating to an identified or identifiable natural person ('the Data Subject'), as further specified in Article 4, paragraph 1, of the GDPR.
Station	a physical location within the infrastructure of Enexis, housing equipment for the transport and/or distribution of electricity and/or gas (e.g. a transformer, switchgear, distribution substation, installation or tool belonging to the electricity grid or gas transport network of Enexis Netbeheer B.V.), as referred to in Article 1(i) of the Electricity Act, Article 1(d) of the Gas Act or the new Energy Act.

Third Party/Parties	a third party is someone engaged by the Counterparty to perform part or all of the Main Agreement, including subcontractors and other contractors. The term "Third Party" also applies when the Counterparty uses goods and/or services of third parties for the benefit of Enexis.

1. PURPOSE, APPLICABILITY AND HIERARCHY

1.1 The purpose of this DV&P Addendum is to supplement the Master Agreement by setting out the minimum Security Measures to be taken and the respective responsibilities of the Parties.

1.2 This DV&P Addendum applies to:

a) All Activities, goods and/or services that the Counterparty performs and will perform, and supplies and will supply, for Enexis under the Master Agreement;

b) All relevant information, processes, goods and services of Enexis that are provided to the Counterparty, or of which the Counterparty becomes aware through the performance of the Master Agreement

1.3 The obligations of the Counterparty under this DV&P Addendum also apply to Enexis Holding N.V. and all companies belonging to its group, where relevant.

1.4 Any deviations from this DV&P Addendum must be agreed upon in writing by the Parties in **Appendix 1 – Agreed Deviations from the DV&P Addendum.**

1.5 In the event of a conflict between this DV&P Addendum and the Master Agreement, the provisions of this DV&P Addendum shall prevail unless the Master Agreement expressly deviates from a provision of this DV&P Addendum.

2. SECURITY POLICY GUIDELINES

2.1 The Counterparty guarantees that all Activities, goods and/or services covered by the Master Agreement, including partial deliveries, comply with the latest applicable laws and regulations relating to Enexis, as well as the latest security standards. This includes, at a minimum:

Legislation

a) the NIS2 Directive as implemented in the Cybersecurity Act;
b) the CER Directive as implemented in the Wwke;
c) the Energy Act, including in particular Article 3.18 of the Energy Act;
d) the Network Code for Digital Security; and
e) the GDPR.

Relevant standards

f) ISO 27001, NIST 800-53, or equivalent standards; and
g) the ICT Security Guidelines from the National Cyber Security Centre.

2.2 The Counterparty further guarantees that all Activities, goods and/or services covered by the Master Agreement, including partial deliveries, comply with the requirements set out in the Appendices.

Appendix 4 - Access Security
Appendix 5 - Encryption & Backups
Appendix 6 - Personal and Physical Security
Appendix 7 - Training and Awareness
Appendix 8 - Patch Management
Appendix 9 - Vulnerability Management
Appendix 10 - Continuity Management
Appendix 11 - Software Development
Appendix 12 - Logging & Security Controls

2.3 The Counterparty has a security quality system that is independently certified (ISO 27001, ISO 9001 or equivalent) and meets the requirements of the Plan-Do-Check-Act cycle. The quality system must aim to protect all Activities, goods and/or services that the Counterparty provides to or uses for Enexis.

Initials Enexis Initials Counterparty

2.4 The Counterparty will implement timely security measures in accordance with ISO 27001 or an equivalent standard. These security measures include technical, physical and organisational measures, implementing at least the following:

a) security risk management, including policies and procedures for assessing the effectiveness of measures;
b) adequate physical protection of relevant buildings and infrastructure;
c) incident prevention, handling and recovery;
d) business continuity measures, including business continuity management, backup management, disaster recovery and crisis management;
e) security of the Counterparty's supply chain (i.e. in relation to Third Parties);
f) security during the acquisition, development and maintenance of network and information systems;
g) employee security awareness and training;
h) logical Access Security, including the use of multi-factor authentication and logging;
i) personnel protection, including physical access and asset protection.

2.5 The Counterparty shall maintain adequate documentation and an overview of all Security Measures referred to in this DV&P Addendum, and shall provide Enexis with a copy upon request.

3. CONFIDENTIALITY AND DATA PROCESSING

3.1 In addition to Article 12.1 of the T&Cs, with regard to Confidential Information and Personal Data, the Counterparty may only use the information for the purposes of performing the Master Agreement. The Counterparty may not disclose, copy or reproduce it, nor use it for its own purposes, without prior permission from Enexis.

3.2 If Enexis grants the Counterparty permission to disclose the information, it may only be disclosed to the individuals to whom permission has been granted, subject to the conditions set out in this DV&P Addendum. The Counterparty must not disclose, copy, reproduce or distribute the information to third parties in any way.

3.3 The obligations under Articles 3.1 and 3.2 of this DV&P Addendum do not apply to information that is already in the public domain at the time it is provided by Enexis, or that must be made public under a statutory provision or regulation. However, this only applies if the Parties have agreed in advance on the proposed form, timeline, nature and purpose of the disclosure.

3.4 Upon Enexis's written request and/or upon termination of the Master Agreement, the Counterparty will return all items containing information provided by Enexis. The Counterparty will return all information as soon as possible and will then delete it irretrievably, unless it is required by law to retain certain information. At the request of Enexis, the Counterparty will provide a written statement confirming that this deletion has been carried out and specifying any information it may still retain by law. The Counterparty will return the information to Enexis in a readable file format, ensuring the integrity and usability of the information.

3.5 This confidentiality obligation takes effect when the Master Agreement is signed and remains in place for ten years after termination.

3.6 If the Parties have entered into a Data Processing Agreement in accordance with Article 22.2 of the GDPR during the term of the Master Agreement, the provisions of the Data Processing Agreement will prevail in the event of any conflict between this DV&P Addendum and that Data Processing Agreement.

3.7 Unless Enexis has granted specific permission to do so, the Counterparty will not process or provide information to countries outside the European Economic Area when performing the Master Agreement. The Counterparty will maintain a central overview of all processing locations in **Appendix 3** – **'Location Information'**. This includes the name, address and country of each processing location, as well as any third-party involvement. In the event of changes, the Counterparty will provide Enexis with a new version as soon as possible, but no later than one month after the change occurs.

3.8 The Counterparty will take appropriate and recognised measures, in accordance with Enexis's instructions, to automatically delete or anonymise outdated information. Where information has not

yet been deleted or anonymised, the Counterparty will mask or pseudonymise it where necessary, in accordance with Guidelines 01/2025 of the European Data Protection Board.

4. AUDIT

4.1 In addition to Articles 11.2 and 11.3 of the T&Cs, Enexis has the right to periodically monitor the Counterparty's compliance with this DV&P Addendum by carrying out an audit with the help of an independent third party. This audit will be performed by an EDP auditor accredited by NOREA or an equivalent organisation. The Counterparty will also enter into contractual arrangements with its suppliers, as designated by Enexis as Critical Third Party, which provide for such an audit right and extend throughout the entire supply chain.

4.2 The Counterparty shall grant the auditor unrestricted access to all systems, documents and locations necessary for a complete and effective audit. The Counterparty shall also provide all relevant information, documentation and reports within a reasonable timeframe. If areas for improvement and/or deficiencies are identified, the Counterparty shall document these and take the necessary corrective and preventive measures. If areas for improvement and/or deficiencies pose a direct risk to Enexis, the Counterparty shall take the necessary corrective and preventive measures within one month at the latest.

4.3 The Parties will treat audit findings and information obtained during the audit as confidential, unless disclosure is required by a Supervisory Authority.

4.4 Enexis will bear the costs of an audit unless the audit reveals that the Counterparty has seriously failed to comply with this DV&P Addendum. In this case, the Counterparty is obligated to reimburse the costs in full or in part.

4.5 Enexis has the right to periodically perform common and generally accepted automated checks on the Counterparty, for example using third-party risk management software based on publicly available sources. These checks will be carried out in such a way as to avoid disrupting the Counterparty's business activities. Enexis will report any deviations impacting the performance of the Master Agreement to the Counterparty. This report will include detailed information about the nature of the deviation, the potential risks and recommendations for corrective measures. Within 30 days of receiving written notification from Enexis, the Counterparty will inform Enexis of the measures it intends to implement to mitigate the identified risks.

4.6 Throughout the term of the Master Agreement, the Counterparty shall hold a valid third-party declaration (Third Party Statement) in accordance with ISAE 3000 or SOC2 Type 2, or an ISO 27001 (or equivalent) certificate relating specifically to the goods, services and/or Activities covered by the Master Agreement. The Counterparty shall provide Enexis with a copy of the relevant certificate within one (1) month of request.

5. COMMUNICATION AND REPORTING

5.1 **Appendix 2 – Contact Persons** – contains a list of individuals who must be contacted by the other Party in specific situations. For example, in the event of an incident referred to in Article 6 of this DV&P Addendum.

5.2 In addition to Article 44.1 of the T&Cs, the Counterparty shall adopt a proactive approach to security matters. The Counterparty shall communicate openly and proactively at least four times a year about security-related developments and threats that may affect Enexis.

5.3 In addition to Article 43 of the T&Cs, the Counterparty will report to Enexis semi-annually on the agreements made in this DV&P Addendum. This report will include, at a minimum:

a) a review of the general conclusions and critical findings of security controls, including penetration tests, internal and external audits, and security logs;
b) a review of any incidents that have occurred;
c) current and anticipated developments regarding work, goods and/or services under the Master Agreement that impact Security and/or certification of the Counterparty;
d) an evaluation of the effectiveness of the Security Measures described in Appendices 4 to 12;
e) relevant threats and risks in the field of security; and

f) updates regarding compliance with laws and regulations.

6. INCIDENT RESPONSE AND REPORTING OBLIGATION

6.1 In addition to Article 38 of the T&Cs, the Counterparty shall actively monitor incidents and any breaches of the Security Measures implemented, reporting the results to Enexis in accordance with this Article.

6.2 At Enexis's request, the Counterparty shall provide all necessary assistance to comply with applicable security laws and regulations. This includes supporting activities and responding to information requests from supervisory authorities, competent authorities and data subjects.

6.3 If an incident occurs, has occurred or is suspected of occurring, the Counterparty is obliged, in addition to Article 38.1 of the T&Cs, to notify the Enexis contact persons listed in **Appendix 2** via the designated means of communication within 12 hours. The notification must include all relevant information about:

a) the estimated time of onset of the incident;
b) if possible, provide a forecast of the recovery time;
c) the nature of the incident;
d) the observed and expected consequences of the incident; and
e) the measures that have been or will be taken to resolve the incident, minimise consequences and/or damage, and prevent recurrence.

6.4 In addition to Article 38.2 of the T&Cs, the Counterparty is obliged to take all reasonable measures to resolve the Incident as quickly as possible, minimise any further consequences and prevent recurrence. The Counterparty will consult with Enexis without delay to reach an agreement on how to proceed.

6.5 The Counterparty will cooperate with Enexis at all times, follow Enexis's instructions and conduct a thorough investigation into the incident. The Counterparty will prepare a report on the incident, including an appropriate response and follow-up steps. The Counterparty will share this report with Enexis as soon as possible.

6.6 In addition to Article 38.3 of the T&Cs, the Counterparty must not provide information about incidents to third parties unless required to do so by law.

6.7 The Counterparty shall maintain a record of incidents and breaches of the Security Measures in place.

7. RELATIONSHIPS WITH THIRD PARTIES

7.1 In addition to Article 20 of the T&Cs, the Counterparty will conduct a due diligence process when selecting a Third Party, to validate its suitability based on its ability to comply with the Security Measures set out in this DV&P Addendum. If a Third Party appears unable to comply with the agreed Security Measures (in whole or in part) and/or poses significant security, continuity and/or privacy risks, it may only be deployed with prior permission from Enexis. During the due diligence process, the Counterparty will determine whether it is a Critical Third Party through a risk assessment, as defined in ISO 27005 or ISO 31000.

7.2 If the Counterparty engages a Third Party to perform (part of) the Master Agreement, the Counterparty will impose on this Third Party at least the same obligations that apply to the Counterparty under this DV&P Addendum, by means of a written agreement as referred to in Article 20.2 of the T&Cs. The Counterparty will remain fully responsible to Enexis for how this Third Party fulfils these obligations.

7.3 In addition to Article 11 of the T&Cs, the Counterparty shall conduct periodic audits and assessments of the Third Party/Parties at least once a year to ensure compliance with the agreed Security Measures. This shall include an audit of the incident response process. The results of these audits and assessments must be documented, and the Counterparty will ensure that any deficiencies are addressed with corrective measures.

7.4 The Counterparty obliges the Critical Third Party/Parties to develop and maintain continuity plans and procedures to ensure continuity and recovery of products and services in the event of an

incident or disruption. Such a continuity plan must meet the requirements set out in **Appendix 10** at a minimum.

7.5 The Counterparty must maintain an up-to-date overview of the Third Party/Parties engaged for the performance of the Master Agreement, including a demarcation of their work from that of other relevant systems and applications.

8. DURATION AND TERMINATION

8.1 The DV&P Addendum will enter into force retroactively, if necessary, once the Parties have signed the Master Agreement legally and validly. The DV&P Addendum will automatically terminate upon termination of the Master Agreement, provided that the provisions of Article 48 of the T&Cs are always complied with.

8.2 The DV&P Addendum provisions that are intended to continue to apply after termination will remain in effect for an additional ten-year period after termination. This applies in any case to Articles 3 (Confidentiality and Data Processing) and this Article.

9. INTERIM TERMINATION, DISSOLUTION AND SUSPENSION

9.1 In addition to Articles 18.1 and 18.4 of the T&Cs, Enexis may suspend, terminate or cancel the Master Agreement with immediate effect and without notice of default or judicial intervention. Enexis may also claim compensation for any damages suffered in the event of:

a) a breach of Article 2, Article 3 and/or Article 6 of this DV&P Addendum by the Counterparty.

9.2 Other than compensation for reasonable and unavoidable costs incurred for goods already in production or work in progress, termination or cancellation of the Master Agreement based on this DV&P Addendum does not entitle the Counterparty to any further compensation.

10. INSURANCE

10.1 The Counterparty has adequate commercial cybersecurity insurance. The insurance policy covers at least [EUR 2,500,000][2] per event. At Enexis's request, the Counterparty will provide the relevant policy conditions and/or proof of insurance coverage.[3]

11. OTHER

11.1 Enexis is entitled to make any changes to the DV&P Addendum that are deemed necessary due to new information, changes in laws and regulations, or changes in circumstances and/or risks.

Explanation: Developments and insights in the field of Cybersecurity are evolving rapidly. This development means that the security measures described in the Appendices are continuously evaluated and further developed. At Enexis, it is standard practice to consult the Counterparty properly before making changes to one of these Appendices

11.2 Changes made by Enexis to this DV&P Addendum entitle the Counterparty to additional payment if the Counterparty can demonstrate that the changes require a level of effort that goes beyond what could reasonably be expected of them.

11.3 Enexis has the right to suspend as referred to in Article 6:52 of the Dutch Civil Code if the Counterparty fails to fulfil its obligations under the DV&P Addendum.

2 The CISO/CLA will consult with an insurance expert to determine this amount.
3 The Master Agreement applies for liability and indemnity.

Thus agreed at <place> and signed:

<date>	<date>
Enexis Personeel B.V./Enexis Netbeheer B.V.]	<name of Counterparty >
<Enexis Signatory>	<Counterparty Signatory >
<Designation>	<Designation>

Initials Enexis

Initials Counterparty

APPENDICES

1. Agreed Deviations from the DV&P Addendum
2. Contacts
3. Locations Information
4. Access Security
5. Encryption and Backups
6. Personnel and Physical Security
7. Training and Awareness
8. Patch Management
9. Vulnerability Management
10. Continuity Management
11. Software Development
12. Logging & Security Controls

Initials Enexis

Initials Counterparty

APPENDIX 1 – AGREED DEVIATIONS DV&P ADDENDUM

The parties have agreed to amend the DV&P Addendum with regard to the following points:

Art.	Text that expires	Replacement text	Reason

Initials Enexis

Initials Counterparty

APPENDIX 2 – CONTACT PERSONS

In the event of a breach and/or incident, or if there is a vulnerability posing a direct risk to Enexis, the Counterparty must report it to **Security@enexis.nl** and contact the Enexis contact persons via the telephone numbers mentioned in Appendix 2. The Counterparty must notify Enexis immediately, but no later than 12 hours after becoming aware of this, via all designated means of communication and provide all relevant information:

Contact information of **Enexis**

Event	Name	Designation	Phone number
Incident and breach	Jeroen Teppema	Chief Information Security Officer	088-8574444
Incident and breach		Contract Manager of Master Agreement	
Incident and breach	Evelyne Hengst-de Greeff	Data Protection Officer	088-8574444

Contact information of **Counterparty**

Event	Name	Designation	Phone number	E-mail
Incident and breach		Chief Information Security Officer		
Incident and breach		Contract Manager of Master Agreement		
Incident and breach		Data Protection Officer		

Initials Enexis

Initials Counterparty

APPENDIX 3 – LOCATION INFORMATION

For the purposes of performing the Master Agreement, the Counterparty uses the following processing locations:

Locations where Counterparty stores and processes information etc.	Locations where Third Parties store or process information, etc.	Explanation
[Country, Address]	[Statutory name, Third Party, Country, Address]	

APPENDIX 4 – ACCESS SECURITY

I. The Counterparty manages access to the ICT Solution and other Counterparty services through technical and organisational measures. This includes, at a minimum:

   a) the use of accounts that can be traced back to user or system activity (i.e. service accounts);
   b) using two-factor authentication based on something you know, something you have, and/or are; and
   c) strong passwords or another widely used, reliable authentication method that can be considered an industry standard.

II. All access to the ICT Solution and other services is managed by the Counterparty via a central authorisation system. This authorisation system ensures consistent and standardised processes for granting and revoking access rights.

III. The Counterparty guarantees the secure and effective implementation and management of a Single Sign-On (SSO) solution within its IT solution, ensuring seamless integration with Enexis's access security system. The Counterparty ensures that the SSO solution complies with relevant industry standards, including protocols such as SCIM, SAML 2.0 and OAuth 2.0.

IV. Access rights within the ICT Solution and other services are assigned according to role. Each role encompasses a set of responsibilities and associated access rights. The Least Privilege Principle forms the basis for defining these roles. The Counterparty maintains a documented overview of the standard roles applied within the ICT Solution and other services.

V. The Counterparty will review access rights to the ICT Solution and other services periodically, at least once every six months. The review will confirm that the assigned rights are correct and still in line with the current roles and responsibilities of the Counterparty's users. Any discrepancies or unauthorised rights will be corrected immediately. The results of this review, including any actions taken, will be documented.

Initials Enexis

Initials Counterparty

APPENDIX 5 – ENCRYPTION AND BACKUPS

I. The Counterparty uses recognised and appropriate encryption methods to protect the confidentiality and integrity of information from unauthorised access, loss or modification. The selected methods comply with applicable industry standards and legal requirements. Encryption keys are stored and managed in accordance with the best practices for key management defined in ISO 11770 (or equivalent), including the regular rotation of keys and auditing. Access to encrypted information is strictly controlled and logged.

II. The information processed and transferred between systems and applications within and outside the Counterparty's network is encrypted in accordance with the requirements set out in the previous article, in order to protect it from interception and manipulation. This includes data transfers via email, APIs, networks and cloud services, among others.

III. In order to combat disasters, the Counterparty will create daily backups of the information, or more frequently if necessary, to enable recovery within the agreed RPO. The Counterparty will take measures to guarantee the availability, integrity and confidentiality of the backups. This includes applying encryption, duplicating the backups to separate physical locations and maintaining contingency locations. The Counterparty will test the backup functionality at least once a year by performing a recovery test and sharing the results with Enexis. If the test is unsuccessful, the Counterparty will implement corrective measures and re-test within one month.

Initials Enexis

Initials Counterparty

APPENDIX 6 – PERSONNEL AND PHYSICAL SECURITY

I. To the extent legally permitted, Enexis may subject the employees of the Counterparty or other third parties engaged by the Counterparty for the performance of the Master Agreement to a security screening. The Counterparty must cooperate fully with this screening. Based on the results, Enexis may refuse to deploy the relevant employee and/or third party for the purposes of the Master Agreement.

II. The following provisions apply if, as part of the Master Agreement, employees and/or third parties of the Counterparty have independent physical access to Enexis locations, including Stations:

a) The Counterparty will only provide access tools related to the provision of services to Enexis to its employees and third parties in accordance with applicable Enexis procedures, and only for as long as they require them to perform their work;
b) any access tools provided by Enexis to the Counterparty's employees, including user accounts, are strictly personal and may not be transferred to another person;
c) for security and safety reasons, employees and third parties of the Counterparty must always be accompanied by an Enexis employee when entering an Enexis location;
d) the Counterparty must comply with the codes of conduct and house rules issued by Enexis and published on its website, which set out how to access Enexis locations and resources safely;
e) if an employee or third party of the Counterparty no longer requires physical access to or use of Enexis resources, including laptops, the Counterparty guarantees that these resources and access means will be returned by that employee or third party in accordance with applicable Enexis procedures, and no later than the day on which they perform their last task for Enexis..

III. If the Counterparty uses IT resources, management and system accounts (or other technical capabilities) made available by Enexis, they shall not use these for any purpose other than performing the Master Agreement. The Counterparty must keep passwords confidential and secure them adequately. They must also limit access to passwords to individuals who require it for the performance of the Master Agreement.

IV. When accessing Enexis applications and systems through federation, the Counterparty employees must register and communicate using business email addresses linked to their organisation. Using personal email addresses, such as Gmail, Hotmail and Yahoo, is not permitted.

Initials Enexis Initials Counterparty

APPENDIX 7 – TRAINING AND AWARENESS

I. The Counterparty will establish a training and awareness programme to periodically educate its employees and third parties on security-related developments, threats and applicable laws and regulations. This training and awareness programme will cover the following topics:

a) recognising and reporting phishing and other digital threats;
b) physical access;
c) securely handling and exchanging confidential information;
d) using strong passwords, two-factor authentication and password managers;
e) secure use of end-user devices (e.g. laptops and phones) and networks;
f) if relevant, secure software development.

II. Depending on the risk profile of the employees and/or third parties involved, and the nature of the work they carry out and/or the goods and/or services they provide, the Counterparty will offer them specific training and awareness programmes.

III. The training shall be provided by an independent and qualified trainer who has:

a) demonstrable experience with best practice in network and information security;
b) knowledge of national, European and international network and information security standards;
c) knowledge of possible measures and solutions for risks referred to in Article 20 of the Cybersecurity Act; and
d) knowledge of network and information security issues at strategic and tactical levels.

APPENDIX 8 – PATCH MANAGEMENT

I. The Counterparty is obliged to periodically make patches and updates available during the term of the Master Agreement, in order to resolve known errors (including security errors) in the ICT Solution and the underlying IT infrastructure, systems and/or information of Enexis.

II. Patching frequency will be risk-based, with a minimum of one patch per month, performed by the Counterparty. In the event of critical security updates, the Counterparty must perform them as soon as possible, but no later than three business days after the update is published. The Counterparty must send Enexis a digital notification at least one business day in advance.

III. The Counterparty must inform Enexis promptly about any planned patches or updates, and provide details of the changes, their potential impact on the ICT Solution and/or services, and the expected interruption. This must be done via digital notification at least seven business days before the intended installation date.

IV. The Counterparty will implement patches and updates within the maintenance windows established in the Service Level Agreement, for example, to minimise the impact on Enexis's operational processes. Exceptions to this are critical patches, which must be installed immediately to ensure the security and integrity of the ICT Solution.

V. The Counterparty must conduct prior to the rollout of the software thorough testing of software patches in a test environment that is representative of the production environment. These tests must cover the following aspects at least:

   a) the (functional) operation of the IT solution;
   b) the impact on existing functionality; and
   c) the security aspects.

VI. If Enexis is responsible for installing patches and updates made available by the Counterparty, Enexis must ensure these patches and updates are installed promptly. The Counterparty must provide Enexis with information about these patches and updates within five business days of their availability.

Initials Enexis

Initials Counterparty

APPENDIX 9 – VULNERABILITY MANAGEMENT

I. The Counterparty is obliged to implement and maintain a vulnerability management programme throughout the term of the Master Agreement. The programme must aim to identify, evaluate and remediate security vulnerabilities in systems, networks and software under the Counterparty's responsibility that are used to perform the Master Agreement, including interfaces with third-party applications and systems.

II. The Counterparty must conduct periodic vulnerability scans and penetration tests on all relevant systems and software. Vulnerability scans must be performed monthly and penetration tests annually, or more frequently if the level of risk requires it.

III. The Counterparty is obliged to evaluate the identified vulnerabilities according to their potential impact and likelihood. This involves classifying the vulnerabilities according to their severity as "critical", "high", "medium" or "low" risk, in accordance with the Common Vulnerability Scoring System (CVSS).

IV. The Counterparty will remedy the identified vulnerabilities within the recovery periods outlined below:

a) Emergency vulnerabilities: as soon as possible;
b) Critical vulnerabilities: within five (5) days of identification;
c) High vulnerabilities: within 21 days of identification;
d) Medium vulnerabilities: within two (2) months of identification;
e) Low vulnerabilities: within a reasonable timeframe, in accordance with the agreed priorities.[4]

V. If Enexis is responsible for resolving vulnerabilities, the Counterparty will inform Exenis in a timely manner about the status of the vulnerabilities. This will include details of the nature and potential impact of the vulnerabilities, as well as the necessary steps to resolve them. The Counterparty will also provide all necessary resources, such as the required software. This will be done via digital notification no later than five business days after identification and evaluation of the vulnerabilities.

4 What qualifies as an Emergency Vulnerability or a Critical Vulnerability etc. is project-specific and must be defined in the Master Agreement.

APPENDIX 10 - CONTINUITY MANAGEMENT

I. Within two (2) months of signing the Master Agreement, the Counterparty must draw up a clear and structured business continuity plan and submit it to Enexis for approval. This plan must include the requirements and processes communicated during the tender process, if applicable. The plan must describe how the agreed work, goods and/or services will continue without significant interruption in the event of failure, termination or breach of contract by a Third Party or Parties. The Counterparty guarantees that the business continuity plan contains the following elements at a minimum:

   a) a complete overview of all essential and relevant processes, systems and Third Parties in the supply chain that are relevant to the Counterparty, detailing their role and the degree of dependency on them for the performance of the Master Agreement with Enexis and with Third Parties involved under Enexis's responsibility;
   b) the critical interfaces between the Counterparty and all Third Parties in the supply chain;
   c) the measures that the Counterparty is taking to ensure the availability, confidentiality and integrity of information, and continuity in the event of a relevant Third Party failing.
   d) the maximum period within which the Counterparty will implement a replacement solution in the event of failure by a relevant Third Party, whether in the form of alternative suppliers or internal capacity; and
   e) procedures for implementing redundancy and regular backups to ensure the availability and confidentiality of backups, including encryption and duplicating backups at separate physical locations;
   f) procedures for restoring systems and data after an incident, including regular testing of the business continuity plan; and
   g) procedures and escalation mechanisms for communicating with Enexis in the event of a disaster.

II. The Counterparty is obliged to periodically test the business continuity plan for suitability, revising it at least once a year and submitting an updated version to Enexis for approval immediately in the event of any changes. In any case, the Counterparty will update this business continuity plan whenever relevant legislation or regulations change or are added to, including any relevant implementing act of the European Commission and relevant guidance from Supervisory Authorities.

III. At the request of one of the Parties, a coordination meeting will be held as soon as possible. Representatives of Enexis, the Counterparty and any relevant Third Parties will attend the meeting. During the meeting, progress, incidents and improvement measures will be discussed.

IV. To manage the risks of ransomware and mitigate attacks, the Counterparty has implemented specific measures, including taking regular backups of critical data and storing it in secure, isolated locations, as well as installing anti-malware and other security software. Should a ransomware attack occur, the Counterparty will activate its continuity plans and establish an incident response team to assess and contain the attack.

APPENDIX 11 - SOFTWARE DEVELOPMENT

With regard to the performance of the Master Agreement by the Counterparty in relation to the development of software, the Parties have agreed as follows:

I. The Counterparty will implement software security policies and procedures throughout the entire Software Development Lifecycle.

II. The Counterparty will establish a secure development environment in which the development, testing, acceptance and production environments are separate, and access to the source code and test data is restricted to employees and/or contractors involved in development. This access is actively managed. Test data does not contain Personal Data and/or Confidential Information, but rather anonymised or fictitious data.

III. The Counterparty will only provide access to the developed software via methods prescribed by Enexis or otherwise agreed upon, and will not implement any covert measures to access Enexis' information and/or systems.

IV. Any web application software used to process information from Enexis and/or third parties will be designed, developed, tested and configured in accordance with the latest secure web application standards, including the OWASP Top Ten and the ICT Security Guideline for Web Applications Infosheet from the National Cyber Security Centre, or other publicly available standards.

V. The Counterparty regularly checks the source code of the developed software for weaknesses, errors and any risks, using manual checks and/or automated tools (code review).

Initials Enexis

Initials Counterparty

APPENDIX 12 – LOGGING & SECURITY CONTROLS

I. The Counterparty will record security activities and events that may affect the integrity, availability or confidentiality of any information, processes, goods or services belonging to Enexis or the Counterparty. The following activities and events will be recorded in security logs at a minimum:

a) attempts to access the system (successful and failed login attempts);
b) changes to system configurations and settings;
c) actions taken by users with elevated privileges;
d) incidents that compromise the security of systems and information; and
e) how recurrence is prevented.

II. The Counterparty undertakes to protect the security logs against unauthorised access, modification, loss or destruction, and to perform regular maintenance on the logging infrastructure to ensure optimal performance and reliability.

III. Security logs are retained for a minimum period of six months, unless an extended retention period is required by law or deemed necessary for ongoing investigations. Once the retention period has elapsed, the data will be deleted securely and responsibly.

IV. The Counterparty must periodically assess the effectiveness of the Security Measures implemented, as well as its ability to recover from incidents, through internal and external audits and reviews. External audits are conducted by independent, qualified auditors. These security audits take various forms, including vulnerability scans of networks and systems, penetration tests, physical security control and access control management. The frequency and nature of these audits are determined based on the sensitivity of the information and continuity risks, and they are performed at least once per year.

V. If any areas for improvement and/or deficiencies are identified, the Counterparty will document them and take the necessary corrective and preventive measures. If any deficiencies pose a direct risk to Enexis, the Counterparty will take the necessary corrective and preventive measures within one month.

VI. The Counterparty uses lessons learned from security controls and external audits to continuously improve its Security Procedures and Security Practices.