Data Processing Agreement

1. **Stichting Veul Diech Good,** having its registered office at Geulhout 12 in Bunde, Netherlands, Chamber of Commerce number 66647908 and duly represented by mr. Anton, Chairman (hereinafter: "**the Controller**");

and

2. **Innovero Software Solutions B.V.,** having its registered office at Rijksstraatweg 713 in Wassenaar, The Netherlands, Chamber of Commerce number 27157981 and duly represented by Mr. M. Rader (hereinafter: "**the Processor**");

Referred to hereinafter jointly as the "**Parties**" and individually as the "**Party**";

WHEREAS:

- On 22/03/2018, the Parties concluded an agreement concerning the use of the Service by the Controller. In performance of the agreement, the Processor processes Personal Data on behalf of the Controller;
- Within the context of the performance of the Agreement, Innovero Software Solutions B.V. is deemed a Processor within the meaning of the GDPR and **Stichting Veul Diech Good** is deemed a Controller within the meaning of the GDPR;
- The Parties want to treat the Personal Data that are or will be processed for the performance of the Agreement with due care and in accordance with the GDPR and other Applicable Legislation and Regulations concerning the Processing of Personal Data.
- In accordance with the GDPR and other Applicable Legislation and Regulations concerning the Processing of Personal Data, the Parties want to lay down their rights and obligations in respect of the Processing of the Data Subjects' Personal Data In Writing in this Data Processing Agreement.

AND AGREE AS FOLLOWS:

CLAUSE 1. DEFINITIONS

The capitalised terms used in this Data Processing Agreement have the meaning given in this article. Where the singular is used in the definition in this article, this is understood to include the plural, and vice versa, unless otherwise is explicitly indicated or shown by the context.

1.1 **GDPR**: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

1.2 **Data Subject**: the identified or identifiable natural person to whom the Personal Data pertain, as referred to in Article 4 at 1) GDPR.

1.3 **Annex**: an annex to this Data Processing Agreement, which forms an integral part of this Data Processing Agreement.

1.4 **Special categories of Personal Data**: Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, and genetic data, biometric data for the purpose of uniquely identifying a natural person, or data concerning health or data concerning a natural person's sex life or sexual orientation, as referred to in Article 9 GDPR.

1.5 **Third Party**: a natural or legal person, public authority, agency or body other than the Data Subject, the Controller or the Processor, or the person who, under the direct authority of the Controller or Processor, is authorised to process Personal Data, as referred to in Article 4 at 10) GDPR.

1.6 **Service**: the forms management system Formdesk to be provided by the Processor to the Controller and has been put into use by the Controller.

1.7 **Personal Data Breach**: (suspicion of) a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed, as referred to in Article 4 at 12) GDPR.

1.8 **Employee**: the employees and other persons engaged by the Processor for whose activities it is responsible and who are engaged by the Processor for the performance of the Agreement.

1.9 **Recipient**: a natural or legal person, public authority, agency or another body, whether or not a Third Party, to whom/which the Personal Data are disclosed, as referred to in Article 4 at 9) GDPR.

1.10 **Agreement**: the agreement concluded between the Controller and the Processor and on the basis of which the Processor processes Personal Data for the Controller for the purpose of the performance of this agreement. With the conclusion of the subscription to the Service and the agreement with the terms and conditions as described on https://en.formdesk.com/general-conditions/ by the Controller, the agreement is concluded.

1.11 **Personal Data**:all information relating to a Data Subject; a natural person who can be directly or indirectly identified, in particular based on an identifier such as a name, an identification number, an online identifier or one or more elements that are characteristic of the physical, physiological, genetic, psychological, economic, cultural or social identity of that natural person, as referred to in Article 4 at 1) GDPR, is deemed identifiable.

1.12 **PIA**: the data protection impact assessment (privacy impact assessment) performed prior to the Processing in respect of the impact of the intended processing activities on the protection of the Personal Data, as referred to in Article 35 GDPR.

1.13 **In Writing**: laid down in writing or by electronic means, as referred to Article 6:277a of the Dutch Civil Code.

1.14 **Sub-processor**: another processor, including but not limited to group companies, sister companies, subsidiaries and auxiliary suppliers, engaged by the Processor to perform specific processing activities at the Controller's expense except for parties with which the Processor has only a technical connection and the Controller has or enters into a direct relationship and listed in annex A.

1.15 **Applicable Legislation and Regulations concerning the Processing of Personal Data**: the applicable legislation and regulations and/or (further) treaties, regulations, directives, decrees, policy rules, instructions and/or recommendations from a competent public body concerning the Processing of Personal Data, also including future amendments of and/or supplements thereto, including laws of the Member States implementing the GDPR and the Telecommunications Act.

1.16 **Supervisory Authority**: one or more independent public bodies responsible for supervising the application of the GDPR, in order to protect the constitutional rights and fundamental freedoms of natural persons in connection with the Processing of their Personal Data and to facilitate the free traffic of Personal Data inside the Union, as referred to in Article 4 at 21) and Article 51 GDPR. In the Netherlands, this is the Dutch Data Protection Authority (Autoriteit Persoonsgegevens).

1.17 **Data Processing Agreement**: the present agreement including Annexes, as referred to in Article 28(3) GDPR.

1.18 **Processing**: any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, as referred to at Article 4 at 2) GDPR.

CLAUSE 2. SUBJECT OF THE Data Processing Agreement

2.1 The Data Processing Agreement forms a supplement to the Agreement and replaces any arrangements agreed earlier between the Parties in respect of the Processing of Personal Data. In the event of any conflict between the provisions of the Data Processing Agreement and the Agreement, the provisions of the Data Processing Agreement prevail.

2.2 The general provisions from the Data Processing Agreement apply for all Processing in the performance of the Agreement. The Processor shall immediately notify the Controller if the Processor has reason to assume that the Processor can no longer comply with the Processing Agreement.

2.3 The Controller shall give the Processor assignments and instructions for processing the Personal Data on behalf of the Controller. The Controller's instructions are formed by the use of the Service and described in more detail in the Data Processing Agreement. The Controller may issue reasonable supplementary or deviating instructions In Writing.

2.4 The Processor shall process the Personal Data exclusively on assignment from the Controller and on the basis of instructions from the Controller. The Processor shall exclusively process the Personal Data in so far as the processing is necessary for the performance of the agreement, and never for its own use, the use of Third Parties and/or other purposes, unless applicable Union law or provisions of Member State law oblige the Processor to perform Processing. In that event, the Processor shall notify the Controller of this provision In Writing prior to the Processing, unless that legislation prohibits such notification for serious reasons of public interest.

2.5 The Processor and the Controller shall comply with the GDPR and other Applicable Legislation and Regulations concerning the Processing of Personal Data. The Processor shall immediately notify the Controller if, in the opinion of the Processor, an instruction from the Controller breaches the GDPR and/or other Applicable Legislation and Regulations concerning the Processing of Personal Data.

2.6 If the Processor determines the purpose and means of the Processing of Personal Data in violation of the Data Processing Agreement and/or the GDPR and/or other Applicable Legislation and Regulations concerning the Processing of Personal Data, the Processor is deemed the Controller for that Processing.

CLAUSE 3. PROCESSING OF PERSONAL DATA

3.1 Before concluding the Data Processing Agreement, the Controller shall inform the Processor in Annex A about the Processing that the Processor conducts in the performance of the agreement.

3.2 Controller bears the responsibility as designer of the forms within the Service, that Annex A complies with the use of the Service and will, where appropriate, provide the Processor with a new Annex A.

3.3 The Processor will not process Personal Data or have it processed by Sub-processors in countries outside the European Economic Area ("EEA") without previous consent In Writing from the Controller.

CLAUSE 4. PROVIDING ASSISTANCE AND COOPERATION

4.1 The Processor shall provide the Controller with all necessary assistance and cooperation in complying with the obligations borne by the Parties on the basis of the GDPR and other Applicable Legislation and Regulations concerning the Processing of Personal Data. The Processor shall provide the Controller with assistance in any event in respect of:

i. Protection of Personal Data;
ii. Performance of verifications and audits;
iii. Performance of PIAs;
iv. Prior consultation with the Supervisory Authority;
v. Compliance with requests from the Supervisory Authority or another public body;
vi. Compliance with requests from Data Subjects;
vii. Reporting Personal Data Breaches.

4.2 Providing assistance and cooperation in respect of compliance with requests from Data Subjects is understood to include, but is not limited to, the following obligations for the Processor:

4.2.1 The Processor shall take all reasonable measures to ensure that the Data Subject can exercise his rights.

4.2.2 If, in relation to the exercise of his rights, a Data Subject contacts the Processor directly, the Processor shall not (substantively) respond - unless expressly instructed otherwise by the Controller - but shall immediately report this to the Controller, with a request for further instructions.

4.3 Providing assistance and cooperation in respect of compliance with requests from the Supervisory Authority or another public body is understood to include, but is not limited to, the following obligations for the Processor:

4.3.1 If the Processor receives a request or order concerning Personal Data from a Dutch and/or foreign public body, including but not limited to a request from the Supervisory Authority, the Processor shall immediately notify the Controller in so far as this is permitted by law. When handling the request or order, the Processor shall observe all of the Controller's instructions and provide to the Controller all reasonably required cooperation.

4.3.2 If the Processor is prohibited by law from complying with its obligations on the basis of Clause 4.3.1, the Processor shall promote the Controller's reasonable interests. This is understood to include, but is not limited to:

4.3.2.1 The Provider shall procure a legal assessment of the extent to which (i) the Processor is required by law to comply with the request or order; and (ii) the Processor is in fact prohibited from complying with its obligations to the Controller based on Clause 4.3.1.

4.3.2.2 The Processor shall only cooperate with the request or order if the Processor is required by law to do so, and the Processor shall object where possible (by legal action) to the request or order or the injunction against informing the Controller in this respect or against following the Controller's instructions.

4.3.2.3 The Processor shall not provide any more Personal Data than strictly necessary to comply with the request or order.

4.2.3.4 If there is processing within the meaning of Clause 3.3, the Processor shall investigate the possibilities for complying with Articles 44 through 46 GDPR.

CLAUSE 5. ACCESS TO PERSONAL DATA

5.1 The Processor shall limit access to Personal Data by Employees, Sub-processors, Third Parties and other Recipients of Personal Data to a necessary minimum.

5.2 The Processor shall exclusively provide access to Employees who must have this access to Personal Data in the performance of the Agreement.

5.3 The Processor shall not provide Sub-processors access to Personal Data without previous consent In Writing from the Controller except Sub-processors as referred to in paragraph 4 of this article. Consent for the engagement of Sub-processors is only given to Sub-processors who are specified in Annex A except Sub-processors as referred to in paragraph 4 of this article.

5.4 If a Sub-processor is used for a specific functionality within the Service, then the use of this specific functionality by the Controller is deemed to provide the Sub-processor with only the personal data that are necessary for the performance of the functionality. The processor is obliged to inform the Controller that a Sub-processor is being used and which Sub-processor is concerned when the relevant functionality is switched on by the Controller.

5.5. The Controller's consent for the engagement of Sub-processors does not prejudice the Processor's obligations ensuing from the Data Processing Agreement, including but not limited to Clause 9. The Controller may withdraw its consent In Writing for the engagement of Sub-processors if the Processor does not satisfy or no longer satisfies the obligations under the Data Processing Agreement, the GDPR and/or other Applicable Legislation and Regulations concerning the Processing of Personal Data.

5.6 The Processor shall impose the obligations included in the Data Processing Agreement on the Employees and/or Sub-processors. The Processor shall ensure that the Employees and/or Sub-processors comply with the obligations included in the Data Processing Agreement by means of an agreement In Writing.

5.7 The Processor shall immediately notify the Controller if the Processor and/or Sub-processors, act in breach of the Data Processing Agreement and/or of the agreement In Writing concluded with the Processor as referred to in Clause 5.6.

5.8 At the Controller's request, the Processor shall provide the Controller with a copy of the agreement In Writing between the Processor and the Sub-processors.

5.9 In respect of the Controller, the Processor remains completely responsible and completely liable for compliance by the Sub-processors engaged by the Processor with the obligations ensuing from the GDPR and/or other Applicable Legislation and Regulations concerning the Processing of Personal Data and the obligations ensuing from the Agreement and the Data Processing Agreement.

CLAUSE 6. SECURITY

6.1 The Processor shall take appropriate technical and organisational measures to safeguard a level of security attuned to the risk, so that the Processing complies with the requirements under the GDPR and other Applicable Legislation and Regulations concerning the Processing of Personal Data, and the protection of the rights of Data Subjects is safeguarded. To this end, the Processor shall take at least the technical and organisational measures included in Annex B.

6.2 In the assessment of the appropriate level of security, the Processor shall take into account the state of the art, the costs of execution, as well as the nature, scope and the risks varying in terms of probability and seriousness to the rights and freedoms of individuals, especially as a result of the accidental or unlawful destruction, loss, alteration or unauthorised provision of or unauthorised access to data that is transferred, stored or otherwise processed.

6.3 The Processor shall lay down its security policy In Writing. At the Controller's request, the Processor shall allow the Controller to inspect the Processor's security policy.

6.4 Association with an approved code of conduct as referred to in Article 40 GDPR or an approved certification mechanism as referred to in Article 42 GDPR can be used to demonstrate compliance with the requirements referred to in this clause.

CLAUSE 7. AUDIT

7.1 The Processor is obliged to periodically have an independent, external expert perform an audit in respect of the Processor's organisation, in order to demonstrate that the Processor complies with the provisions of the Agreement, the Data Processing Agreement, the GDPR and other Applicable Legislation and Regulations concerning the Processing of Personal Data.

7.2 The Processor shall perform a periodic audit as referred to in Clause 7.1 at least once every two years. If Special Categories of Personal Data are processed, the Processor shall perform a periodic audit as referred to in Clause 7.1 at least once every year.

7.3 At the Controller's request, the Processor is obliged to make the findings of the independent, external expert available in the form of a statement in which the expert gives an opinion on the quality of the technical and organisational security measures taken by the Processor in respect of the Processing conducted by the Processor on behalf of the Controller.

7.4 At its request, the Controller has the right to have an audit in respect of the Processor's organisation performed by a (legal) person authorised by the Controller, in order to demonstrate that the Processor complies with the provisions of the Agreement, the Data Processing Agreement, the GDPR and other Applicable Legislation and Regulations concerning the Processing of Personal Data.

7.5 The costs of the periodic audit are at the expense of the Processor. The costs of the audit at the Controller's request are at the Controller's expense. This provision does not prejudice the Controller's other rights, including the right to damages.

7.6 If it is established during an audit that the Processor has failed to comply with the provisions of the Agreement and/or the Data Processing Agreement and/or the GDPR and/or other Applicable Legislation and Regulations, the Processor shall immediately take all measures that are reasonably necessary to ensure the Processor's compliance with these as yet. The accompanying costs are at the Processor's expense.

CLAUSE 8. PERSONAL DATA BREACH

8.1 Without unreasonable delay and no later than within 24 hours after discovery, the Processor shall notify the Controller of a Personal Data Breach or a reasonable suspicion of a Personal Data Breach. The Processor shall notify the Controller via the Controller's contact and contact details included in Annex A. The Processor warrants that the information provided is complete, correct and accurate.

8.2 If and in so far as it is not possible for the Processor to simultaneously provide all of the information, the information may be provided to the Controller step-by-step without unreasonable delay and no later than within 24 hours after the discovery.

8.3 The Processor has organised adequate policy and adequate procedures to detect Personal Data Breaches at the earliest possible stage, to notify the Controller of this no later than within 24 hours, to adequately and immediately respond to this, to prevent or limit (further) unauthorised disclosure, alteration and provision or otherwise unlawful Processing, and to prevent repetition of the same. At the Controller's request, the Processor shall provide information about and allow inspection of this policy organised by the Processor and these procedures organised by the Processor.

8.4 The Processor shall maintain a register In Writing of all Personal Data Breaches that relate to or are connected with the (performance of the) Agreement, including the facts regarding the Personal Data Breach, its consequences and the corrective measures taken. At the Controller's request, the Processor shall provide the Controller with a copy of this register.

CLAUSE 9. CONFIDENTIALITY OF PERSONAL DATA

9.1 All Personal Data are qualified as confidential and must be treated as such.

9.2 The Parties shall keep all Personal Data confidential and shall not disclose them in any way, either internally or externally, except in so far as:

i. (i) Disclosure and/or provision of the Personal Data is necessary in the context of the performance of the Agreement or the Data Processing Agreement;
ii. (ii) Any mandatory statutory provision or court decision requires the Parties to disclose and/or provide the Personal Data, in which case the Parties shall first notify the other Party of this;
iii. (iii) Disclosure and/or provision of the Personal Data takes place with prior consent In Writing from the other Party.

9.3 Breach of Clause 9.1 and/or Clause 9.2 is deemed a Breach of Personal Data.

CLAUSE 10. LIABILITY AND INDEMNIFICATION

10.1 The Processor is liable for all damage ensuing from or in connection with the failure to comply with the Data Processing Agreement and/or the GDPR and/or other Applicable Legislation and Regulations concerning the Processing of Personal Data by Processor.

10.2 The Processor indemnifies the Controller against all claims, penalties and/or measures by third parties, including Data Subjects and the Supervisory Authority, lodged against or imposed on the Controller due to breach of the Data Processing Agreement and/or the GDPR and/or other Applicable Legislation and Regulations concerning the Processing of Personal Data by the Processor and/or Sub-processors.

10.3 The compensation for the damage resulting from the liability is limited to an amount of € 500,000 per claim and € 1,000,000 per year.

10.4 The Processor shall ensure sufficient coverage of the liability by means of liability insurance. At the Controller's request, the Processor shall allow the Controller to inspect the Processor's (policy for this) liability insurance.

CLAUSE 11. CHANGES

11.1 The Processor is obliged to immediately notify the Controller of changes in the performance of the Agreement and the performance of the Data Processing Agreement that concern the Processing of Personal Data. This is understood to include, but is not limited to:

i. Changes that (may) affect the Personal Data (categories) to be processed;
ii. The engagement of other Sub-processors;
iii. Changes in the transfer of Personal Data to third countries and/or international organisations.

11.2 If a change concerning the Processing of Personal Data or an audit gives cause to do so, the Parties shall consult upon the Controller's first request regarding the changes in the Data Processing Agreement.

11.3 The Processor is only entitled to implement a change in the performance of the Agreement, a change in the performance of the Data Processing Agreement and/or a change resulting in amending Annex A if the Controller has given previous consent for such change(s) In Writing.

11.4 Changes that concern the Processing of Personal Data may never result in the Controller being unable to comply with the GDPR and/or other Applicable Legislation and Regulations concerning the Processing of Personal Data.

11.5 In the event of invalidity or avoidability of one or more of the provisions of the Processors Agreement, the other provisions continue to apply in full.

CLAUSE 12. TERM AND TERMINATION

12.1 The term of the Data Processing Agreement is the same as the term of the Agreement. The Data Processing Agreement cannot be terminated separately from the Agreement. Upon termination of the Agreement, the Data Processing Agreement terminates by operation of law, and vice versa.

12.2 The Controller is entitled to cancel the Data Processing Agreement if the Processor does not or can no longer comply with the Data Processing Agreement, the GDPR and/or other Applicable Legislation and Regulations concerning the Processing of Personal Data, without the Processor being entitled to any damages. When cancelling, the Controller shall observe a reasonable notice period, unless the circumstances justify immediate cancellation.

12.3 Within one month after the Agreement ends, the Processor shall destroy all Personal Data. All existing (other) copies of Personal Data, whether or not held by Sub-processors, will also be permanently deleted, unless storage of the Personal Data is mandatory under Union or Member State law.

12.4 At the Controller's request, the Processor shall confirm In Writing that the Processor has satisfied all obligations under Clause 13.3.

12.5 The Processor shall bear the costs for the destruction.

12.6 Obligations under the Data Processing Agreement that are intended by their nature to continue after termination of this Data Processing Agreement will continue to apply after termination of the Data Processing Agreement.

CLAUSE 13. APPLICABLE LAW AND DISPUTE RESOLUTION
13.1 The Data Processing Agreement and its performance are governed by the laws of the Netherlands.

13.2 All disputes arising between the Parties in connection with the Data Processing Agreement shall be submitted to the competent court in the place in which the Controller has its registered office.

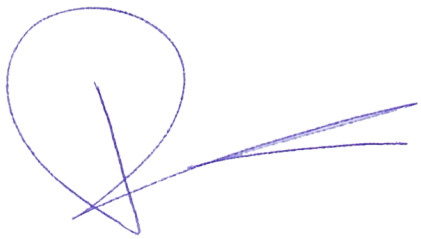
THUS AGREED BY THE PARTIES:

On behalf of

the Controller
Bunde, Netherlands 30-03-18
Stichting Veul Diech Good

mr. Anton
Chairman

the Processor
Wassenaar, The Netherlands 03-04-18
Innovero Software Solutions B.V.



Dhr. M. Rader
Managing Director

ANNEX A: Specifications of the Processing of Personal Data
Version number: 1, Last modification Date: 30/03/2018

Purposes of the Processing
Voor alle acties die de stichting uitvoert (zoals kerstacties, dagje uit enz.) individuele hulpaanvragen.

Categories Data Subject Involved
Onze vrijwilligers, bezoekers aan onze website, cliënten.

(categories) Personal data

Wij verwerken de volgende persoonsgegevens:
- Voor- en achternaam;
- Geslacht;
- Incidenteel uw BSN nummer (dit is nodig indien wij u helpen inzake bijvoorbeeld inkomensproblematiek);
- Adres: straat, postcode en woonplaats;
- Telefoonnummer;
- Emailadres;
- Gegevens over uw inkomen (bij de jaarlijkse kerstactie en een hulpaanvraag).
- Op verzoek verwerken we ook gegevens over lichamelijke beperkingen. Dit zijn zaken waarmee we in de praktijk (functioneel) rekening moeten houden, om de juiste hulp aan u te kunnen bieden. Met andere woorden, uw beperking(en) registreren we op naam, niet op inhoud of detail.

- Registraties:
- Wij registreren aan welke acties/projecten u meedoet, die de stichting organiseert;
- Wij registreren gespreksverslagen, telefoontjes en andere zaken om uw gegevens up to date te houden;
- Wij registreren hulpaanvragen;
- Wij registeren (met een schriftelijke, door u ondertekende verklaring) datgene wat u van de stichting ontvangen heeft (bijvoorbeeld witgoed of andere zaken).
- Wij registeren, indien u zich aanmeldt voor de nieuwsbrief, of indien u zich aanmeldt als vrijwilliger.

Sub-processors
The Processor has permission from the Controller to deploy the following Sub-processors in the execution of the Service:

1.
Organization: Secure Cyber Communications B.V.
Purpose of processing: Monitoring traffic through the firewalls for threats.
Country: the Netherlands

Technical connectors
Formdesk Functionalities in which the Processor places technical connectors with third parties with which the Controller has or starts a direct relationship and who are therefore also a Processor for the Controller. As a result, these parties are not considered as Sub-processors.

- Online payment - offers the Controller the possibility to have the person that fills in the form (Data Subject) pay after submitting the form. For this purpose, the Processor connects with various national and international payment service providers at the choice of Controller.
- SMS – offers the Controller the possibility to send SMS messages after the Data Subject has filled in a form, as verification or as authentication (as 2nd factor with 2 factor authentication). For this purpose, the Processor connects with various national and international SMS providers at the choice of Controller.
- Webhooks – offer the Controller the possibility to make a connection and exchange data with third parties at the option of Controller by means of a standard protocol.
- Digital signing - offers the Controller the opportunity to have the Data Subject sign a completed form with the help of DigiD or eHerkenning. For both DigiD and eHerkenning an acceptance process precedes prior to the use of DigiD or eHerkenning. Authentication with eHerkenning - offers the Controller the opportunity to have the Data Subject concerned log in with his or her eHerkenning Id before a form can be completed. An acceptance process precedes the use of eHerkenning.

Contact details in the event of Personal Data Breaches

Controller	Processor
Name: Anton Vegers	Name: dhr. M. Rader
Position: Chairman	Position: Managing Director
Email: info@stichtingveuldiechgood.nl	Email: m.rader@formdesk.com
Telephone: 06-29460091	Telephone: +31 85 4014680

ANNEX B: Security Measures

Management of Information Security;
• Processor consciously deals with information security. To this end, the organization has, among other things, a formal information security policy.
• The information security policy is reviewed at scheduled intervals or when significant changes occur to ensure that it is constantly appropriate, adequate and effective.
• All responsibilities in information security are defined and assigned.

Access control;
• Authorizations on the network and business-critical applications are periodically checked for correctness.
• The number of users with administrator privileges (in the relevant applications) is limited and in accordance with job level and responsibilities.
• The processor has insight into the ways in which access can be gained to the data, outside the application, eg via ODBC links or DBA maintenance work on the database.
• Access to the program source code is limited.

Personnel aspects;
• Verification of the background of all candidates for employment is carried out in accordance with relevant legislation and regulations and is proportional to the business requirements, the classification.
• The management requires all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.
• All employees and contractors have signed a confidentiality agreement.
• Processor has a procedure that ensures that user accounts are blocked (in time) and / or deleted upon termination of employment.

Physical security;
• The processor has taken physical measures to protect its information systems against unauthorized access. The number of employees with access to the server room is limited and in accordance with job level and responsibilities.
• Media is removed in a safe and secure way if it is not needed for longer, according to formal procedures.
• Media containing information are protected against unauthorized access, misuse or corruption during transport.
• Equipment is properly maintained to ensure its continuous availability and integrity.

Operations management;
• Processer has a formal change management process, ensuring that only authorized and tested changes are taken into production. This is laid down in a procedure.
• The processor has taken measures to prevent computer viruses and / or worms from infecting the company network and systems.
• The processor has a back-up & restore procedure to ensure that, in view of possible emergencies, up-to-date backups of both program files and data files are available.
• In order to protect the information transport, which runs through all types of communication facilities, formal policy rules, procedures and control measures for transport apply.
• Information included in electronic messages is appropriately protected.
• Information forming part of application transactions is protected to prevent incomplete transfer, erroneous routing, unauthorized change of messages, unauthorized disclosure, unauthorized duplication or playback.
• Rules have been laid down for the development of software and systems and these are applied to development activities within the organization.