DEPOSIT AGREEMENT

dated 4 May 2021

between

AEGON BANK N.V.
as Issuer, Transferor and Originator

and

AEGON HYPOTHEKEN B.V.
as Servicer and Originator

and

AEGON LEVENSVERZEKERING N.V.
as Originator

and

AEGON SB COVERED BOND COMPANY B.V.
as CBC

and

STICHTING SECURITY TRUSTEE AEGON SB COVERED BOND COMPANY
as Security Trustee

and

NAUTADUTILH N.V.
as the Agent

TABLE OF CONTENTS

THIS DEPOSIT AGREEMENT is dated 4 May 2021, and made between:

1. **AEGON BANK N.V.**, a public limited liability company (*naamloze vennootschap*) organised under the laws of the Netherlands and established in Amsterdam, the Netherlands;

2. **AEGON HYPOTHEKEN B.V.**, a private company with limited liability (*besloten vennootschap met beperkte aansprakelijkheid*) organised under the laws of the Netherlands and established in The Hague, the Netherlands;

3. **AEGON LEVENSVERZEKERING N.V.**, a public limited liability company (*naamloze vennootschap*) organised under the laws of the Netherlands and established in The Hague, the Netherlands;

4. **AEGON SB COVERED BOND COMPANY B.V.**, a private company with limited liability (*besloten vennootschap met beperkte aansprakelijkheid*) organised under the laws of the Netherlands, and established in Amsterdam, the Netherlands;

5. **STICHTING SECURITY TRUSTEE AEGON SB COVERED BOND COMPANY**, a foundation (*stichting*) organised under the laws of the Netherlands, and established in Amsterdam, the Netherlands; and

6. **NAUTADUTILH N.V.**, a public company (*naamloze vennootschap*) organised under Dutch law and established in Rotterdam, the Netherlands, hereinafter referred to as the "**Agent**".

WHEREAS:

(A) The Transferor and the Originators have entered into a covered bond programme pursuant to which the Issuer will issue Covered Bonds from time to time (the "**Programme**").

(B) As part of the Programme, the Transferor, the Originators and the CBC have, among others, entered into the Guarantee Support Agreement dated 4 May 2021 and as the same may be further amended, restated, supplemented or otherwise modified from time to time, pursuant to which, in consideration of the CBC issuing the Guarantee and so as to enable the

CBC to meet its obligations under the Guarantee, the Transferor will transfer and assign to the CBC Eligible Assets from time to time.

(C) Also as part of the Programme, the CBC and the Security Trustee have entered into a security trustee receivables pledge agreement dated 4 May 2021 (the "**Pledge Agreement**"), pursuant to which the CBC will pledge the Mortgage Receivables, the NHG Advance Rights and the Beneficiary Rights to the Security Trustee.

(D) The details of the Mortgage Receivables are set out on the List of Mortgage Loans (whether or not in electronic form), attached to the relevant Deed of Assignment and Pledge and updated on a quarterly basis.

(E) In connection with the General Data Protection Regulation, the List of Mortgage Loans excludes (a) the name and address of the debtors under the relevant Mortgage Receivables and (b) the address of the property encumbered with the mortgage right (the "**Personal Data**").

(F) The Transferor, the Servicer, the CBC and the Security Trustee wish to deposit with the Agent the Escrow List of Loans, which list, for the avoidance of doubt, includes (a) the name and address of the debtors under the relevant Mortgage Receivables and (b) the address of the property encumbered with the mortgage right, if different from (a) (as further described in Clause 2 below), which list will only be released on the terms and subject to the conditions as set out in this Deposit Agreement.

(G) The Agent has agreed to accept such deposit of the Escrow List of Loans in accordance with the terms hereof.

IT IS AGREED as follows:

1. INTERPRETATION

1.1 In this Agreement (including its recitals), except so far as the context otherwise requires, words, expressions and capitalised terms used herein and not otherwise defined or construed herein shall have the same meaning as defined or construed in the master definitions agreement signed on 4 May 2021 by, amongst others, the Transferor, the Security Trustee and the CBC, as the same may be further amended, restated, supplemented or

otherwise modified from time to time (the "**Master Definitions Agreement**"). The rules of usage and of interpretation as set forth in the Master Definitions Agreement shall apply to this Agreement, unless otherwise provided herein.

1.2 The expression "**Agreement**" shall herein mean this Deposit Agreement including its annexes.

1.3 This Agreement expresses and describes Dutch legal concepts in English and not in their original Dutch terms. Consequently, this Agreement is concluded on the express condition that all words, terms and expressions used herein shall be construed and interpreted in accordance with Dutch law.

1.4 For the avoidance of doubt, any amendment, restatement, supplement or other modification to any of this Agreement, including, for the avoidance of doubt its Annexes, or, by reference, to the Master Definitions Agreement shall only be binding on the Agent, if the Agent has given its prior written consent thereto.

2. DEPOSIT

2.1 After each transfer of the relevant Mortgage Receivables by the Transferor to the CBC or after each retransfer of the relevant Mortgage Receivables to the Transferor having taken place in accordance with the Guarantee Support Agreement, the updated Escrow List of Loans will be deposited by the Servicer with the Agent and the Servicer will in accordance with Clause 13.2 and 13.3 of the Servicing Agreement deposit on each Transfer Date and on a quarterly basis with the Agent the Escrow List of Loans in electronic file in MS Word format, MS Excel format or PDF format (or a similar or other software application available to the Agent), which will replace all earlier Escrow Lists of Loans. The Agent shall proceed with such replacement upon receipt by the Agent of a written instruction to that effect addressed by the Administrator to the Agent.

2.2 The Agent may file the received Escrow List of Loans (in the form of electronic documents, such as documents in the form of a Microsoft Word Document, Microsoft Excel document or PDF document) in its electronic document management system.

2.3 The Agent will procure that its notarial department will perform its functions under this Agreement.

3. RELEASE OF DOCUMENTS

The Agent shall as soon as reasonably practicable release the Escrow List of Loans to the CBC and the Security Trustee, subject to the condition precedent of receipt by the Agent of a (photo) copy of a statement addressed by the CBC or the Security Trustee to the Servicer and the Transferor in the form of Annex I hereto, in which the CBC or the Security Trustee informs the Servicer and the Transferor that, in respect of Mortgage Receivables originated by Aegon Bank, a Security Trustee Pledge Notification Event and an Assignment Notification Event has occurred and, in respect of Mortgage Receivables originated by Aegon Leven or Aegon Hypotheken, a Security Trustee Pledge Notification Event and both an Assignment Notification Event and an Originator Assignment Notification Event in respect of Aegon Leven or Aegon Hypotheken, respectively, have occurred and that the condition to release the relevant Escrow List of Loans has been fulfilled. In such event, the Agent shall only release the Escrow Lists of Loans to the CBC and Security Trustee, after the Agent and the recipients have entered into a data processing agreement as required by the General Data Protection Regulation.

4. DUTIES OF THE AGENT/EXCLUSION OF LIABILITY/ INDEMNIFICATION

4.1 The Agent shall perform only such duties as are expressly set forth in this Agreement and shall not be obliged to recognise directions or instructions not specifically set forth herein. The Agent's duties shall be solely mechanical and administrative in nature.

4.2 The Agent shall not be liable for any mistake of fact or error of judgment by it or for any other acts or omissions by it of any kind whatsoever unless caused by gross negligence or wilful misconduct and shall be entitled to rely upon any (photo copy of a) written statement or notice and signatures thereon presented to him in connection with this Agreement.

4.3 The Agent shall have no obligation to ascertain whether any Escrow List of Loans is deposited on a quarterly basis and shall not be responsible for

any failure of the Transferor and/or the Servicer to deposit any such Escrow List of Loans.

4.4 The Transferor, the Security Trustee and the CBC hereby irrevocably and unconditionally agree with the Agent that they shall jointly and severally indemnify the Agent for any loss, damage or other liability incurred by the Agent in connection with or as a result of his acting as Agent.

4.5 The Transferor, the Originators and the Agent have agreed amongst themselves only, to the agreements, rights and obligations vis-à-vis the Agent respectively the Transferor and the Originators, as set out in the Data Processing Agreement as set out in Annex III.

5. TERMINATION

5.1 This Agreement shall terminate and be of no further force or effect:

(a) in the event that the CBC no longer holds any Mortgage Receivables and notice thereof has been given by the Transferor to the Agent substantially in the form of **Annex II** hereto; or,

(b) in the event of a release by the Agent of the Escrow List of Loans pursuant to Article 3 of this Agreement.

5.2 In the event that this Agreement is terminated in accordance with Article 5.1 of this Agreement, the Escrow List of Loans shall be placed in a dedicated folder in the Agent's document management system and will be deleted out of the electronic document management system of the Agent as soon as possible.

6. COSTS AND FEES

The Transferor agrees to pay the Agent (i) an up-front total fee of EUR 1,000 exclusive of VAT (if any), and (ii) an annual deposit fee of EUR 1,000, exclusive of VAT (if any), for the performance by the Agent of the services under or in connection with this Agreement. The annual deposit fee shall be payable for the first time one year after the date of this Agreement and annually thereafter. Furthermore, the Transferor agrees to

reimburse the Agent for all time spent at the then prevailing hourly rates of the Agent and for all disbursements incurred by the Agent in the performance of its duties hereunder, which amounts shall be paid by the Transferor to the Agent quarterly in arrears.

7. NO DISSOLUTION, NO NULLIFICATION

To the extent permitted by law, the parties hereby waive their rights pursuant to Articles 6:265 to 6:272 inclusive of the Netherlands Civil Code to dissolve (*ontbinden*), or demand in legal proceedings the dissolution (*ontbinding*) of, this Agreement. Furthermore, to the extent permitted by law, the parties hereby waive their rights under Article 6:228 of the Netherlands Civil Code to nullify, or demand in legal proceedings the nullification of, this Agreement on the ground of error (*dwaling*).

8. GOVERNING LAW AND JURISDICTION

This Agreement and any non-contractual obligations arising out of or in relation to this Agreement shall be governed by and construed in accordance with Dutch law. Any disputes arising out of or in connection with this Agreement including, without limitation, disputes relating to any non-contractual obligations arising out of or in connection with this Agreement shall be submitted to the exclusive jurisdiction of competent courts in Amsterdam, the Netherlands.

9. MISCELLANEOUS

9.1 Each party to this Agreement is aware of the fact that the Agent (i.e. NautaDutilh N.V.), is the firm that has advised the Transferor and the CBC in respect of, *inter alia*, the Guarantee Support Agreement and this Agreement, and any other document relating to the Programme. Each party to this Agreement (except the Agent) explicitly agrees that the CBC is assisted by the Agent in relation to this Agreement and any agreements that may be concluded, or disputes that may arise, in connection therewith or in connection with the Programme.

9.2 In case a Borrower makes use of his right to request access to personal data in accordance with Article 15 of the General Data Protection Regulation,

each of the Transferor, the CBC, the Security Trustee and the Servicer who has been requested by a Borrower to grant access to personal data will use all reasonable endeavours to ensure that the relevant controller (*verwerkingsverantwoordelijke*) can comply with such request.

9.3 The Parties hereby confirm that in respect of Mortgage Receivables originated by Aegon Bank, until a Security Trustee Pledge Notification Event and an Assignment Notification Event have occurred and, in respect of Mortgage Receivables originated by Aegon Leven or Aegon Hypotheken, until a Security Trustee Pledge Notification Event and both an Assignment Notification Event and an Originator Assignment Notification Event in respect of Aegon Leven or Aegon Hypotheken, respectively, have occurred and the relevant Escrow List of Loans has been released, the Transferor determines the purposes and means of the processing of personal data and after such event the Transferor and, to the extent any of the CBC and/or Security Trustee is processing the personal data, each of the CBC and/or Security Trustee are deemed a controller and not joint controllers, within the meaning of the General Data Protection Regulation.

9.4 Irrespective of any provision to the contrary in this Agreement or any other Transaction Document, none of the parties hereto shall have an obligation under this Agreement or any other Transaction Document to provide any personal information or personal data as a result of which such party, in its reasonable opinion, would violate any of the provisions or requirements of the General Data Protection Regulation.

9.5 If at any time this Agreement and the arrangements laid down herein need to be modified as a result of the General Data Protection Regulation, the Transferor, the CBC, the Security Trustee and the Servicer will cooperate and agree to any such modification in order to enable each of the parties to comply with any requirements which apply to it under the General Data Protection Regulation.

(*signature page follows*)

SIGNATURES

AEGON BANK N.V.

by :	by :
title : proxy holder	title : proxy holder

AEGON SB COVERED BOND COMPANY B.V.

by :
title : proxy holder

AEGON HYPOTHEKEN B.V.

by :
title : proxy holder

AEGON LEVENSVERZEKERING N.V.

by :
title : proxy holder

STICHTING SECURITY TRUSTEE AEGON SB COVERED BOND COMPANY

_____

by :
title : proxy holder

NAUTADUTILH N.V.

_____

Agent

ANNEX I

[letterhead Aegon SB Covered Bond Company B.V. / Stichting Security Trustee Aegon SB Covered Bond Company]

To: [Aegon Bank N.V.] [Aegon Hypotheken B.V.]
Attention: [...]

[Date]

Dear Sirs,

Guarantee Support Agreement dated 4 May 2021

Capitalised terms used in this letter have, unless expressly defined otherwise herein, the same meaning as in the Master Definitions Agreement dated 4 May 2021 and as the same may be further amended, restated, supplemented or otherwise modified from time to time. We refer to the Guarantee Support Agreement made between (1) Aegon SB Covered Bond Company B.V., (2) Aegon Bank N.V. (3) Aegon Levensverzekering N.V., (4) Aegon Hypotheken B.V. and (5) Stichting Security Trustee Aegon SB Covered Bond Company.

We hereby inform you that a Notification Event has occurred and that the condition to release the Escrow List of Loans has been fulfilled. We therefore request the Agent to release the Escrow List of Loans to [Aegon SB Covered Bond Company B.V. / Stichting Security Trustee Aegon SB Covered Bond Company].

Yours faithfully,

[Aegon SB Covered Bond Company B.V. / Stichting Security Trustee Aegon SB Covered Bond Company]

ANNEX II

[letterhead Aegon Bank N.V.]

To: NautaDutilh N.V.
Attention:

[Date]

Dear Sir,

Deposit Agreement dated 4 May 2021

Capitalised terms used in this letter have, unless expressly defined otherwise herein, the same meaning as in the Master Definitions Agreement dated 4 May 2021 and as the same may be further amended, restated, supplemented or otherwise modified from time to time. We refer to the Deposit Agreement (the "**Agreement**") dated 4 May 2021 and as the same may be further amended, restated, supplemented or otherwise modified from time to time and made between (1) Aegon SB Covered Bond Company B.V., (2) Aegon Bank N.V., (3) Aegon Levensverzekering N.V., (4) Aegon Hypotheken B.V., (5) Stichting Security Trustee Aegon SB Covered Bond Company and (6) NautaDutilh N.V.

Pursuant to Clause 5.1 (a) of the Agreement we hereby inform you that Aegon SB Covered Bond Company B.V. no longer holds any Mortgage Receivables.

Yours faithfully,

Aegon Bank N.V.

ANNEX III

DATA PROCESSING AGREEMENT

1. NautaDutilh N.V., a company organised under the laws of the Netherlands, whose corporate seat is at Rotterdam, the Netherlands; hereinafter referred to as "**Processor**";

2. **Aegon Bank N.V.,** a public company (*naamloze vennootschap*) organised under Dutch law, and with its registered office in Amsterdam, the Netherlands;

3. **Aegon Hypotheken B.V., a private company with limited liability (*besloten vennootschap met beperkte aansprakelijkheid*) organised under the laws of the Netherlands and established in The Hague, the Netherlands;**

4. **Aegon Levensverzekering N.V, a public company (*naamloze vennootschap*) organised under Dutch law, and with its registered office in The Hague, the Netherlands;**

(each of the parties under 2, 3 and 4 hereinafter referred to as a "**Controllers**")

WHEREAS

1. Reference is made to the deposit agreement, made between (a) the Controllers as the issuer, originator and transferor and servicer, respectively, the Processor as agent and other parties (the "**Deposit Agreement**").

2. Under the Deposit Agreement, the Processor (i.e. the persons acting under its authority as specified in Annex B (Details of Processing)) provides or shall provide Services to the Controllers. The provision of the Services involves the Processing of Personal Data by the Processor on behalf of the Controllers. The Parties wish to comply with Data Protection Laws and enter into this DPA as required thereunder.

3. This DPA shall form an integral part of the Deposit Agreement.

IT IS AGREED as follows:

1. DEFINITIONS AND INTERPRETATION

1.1 Definitions

a. Capitalised terms and expressions have the meaning given to them in Annex A (*Definitions*).
b. Capitalised terms not otherwise defined herein shall have the meaning given to them in the Deposit Agreement.

1.2 Construction and interpretation

a. A reference to an agreement is a reference to such agreement as amended, restated, modified, revoked or rescinded from time to time.
b. The word "includes" and its derivatives means "includes, but is not limited to" and corresponding derivative expressions.
c. Words denoting the singular shall include the plural and vice versa.
d. The section headings used in this DPA are for convenience of reference only and are not to affect its construction or to be taken into consideration in its interpretation.

2. DESCRIPTION OF THE PROCESSING

2.1 Subject-matter, duration and nature of the Processing

a. The subject-matter of the Processing of Personal Data by the Processor on behalf of the Controllers is the provision of the Services by the Processor to the Controllers.
b. The Personal Data shall be processed by the Processor for the duration of the Services and this DPA, as further described in Clause 12 (*Term*) of this DPA. The Processor shall comply with the provisions of this DPA for as long as Personal Data are Processed by the Processor on behalf of the Controllers.
c. The Personal Data shall be Processed by the Processor insofar as necessary for the provision of the Services and as provided for under this DPA, the Deposit Agreement or as otherwise agreed in writing between the Parties, as further described in Annex B (*Details of*

Processing).

2.2 Types of Personal Data and categories of Data Subjects

a. On behalf of the Controllers, the Processor Processes the Personal Data which are necessary for the provision of the Services. These include the types of Personal Data as set out in Annex B (*Details of Processing*).
b. The categories of Data Subjects whose Personal Data are Processed by the Processor on behalf of the Controllers under this DPA are set out in Annex B (*Details of Processing*).

3. INSTRUCTIONS AND PURPOSE

3.1 Processor

The Processor acts as a processor (*verwerker*) as defined in the GDPR and Data Protection Laws.

3.2 Documented Instructions and Purpose

a. The Processor shall Process the Personal Data in accordance with the documented instructions of the Controllers, including as described in the Deposit Agreement and this DPA, and this is the sole purpose for which the Processor may Process the Personal Data. The Controllers confirm that the Processor's obligations under the Deposit Agreement and this DPA, constitute the instructions to be followed by the Processor.
b. Notwithstanding a. above, the Processor may also Process Personal Data as required by applicable EU or EU Member State law. In case of such requirement of EU or EU Member State law, the Processor shall inform the Controllers of that legal requirement before Processing the Personal Data, unless that law prohibits such information to be provided to the Controllers on important grounds of public interest.
c. The Processor shall immediately inform the Controllers if, in its opinion, any instruction given by the Controllers infringes any Data Protection Laws.

3.3 Lawful Processing

The Controllers warrant and guarantee that (i) they have lawfully obtained the Personal Data, (ii) the Processing of the Personal Data by the Processor is lawful and has a specific purpose, (iii) any required notices have been made, and (iv) consent has been obtained (where applicable) or there is another appropriate lawful processing ground enabling (a) the Controllers to transfer the Personal Data to the Processor and the Processor to receive the Personal Data from the Controllers, and (b) the Processor to lawfully Process the Personal Data.

4. NON-DISCLOSURE AND CONFIDENTIALITY

4.1 Non-disclosure and confidentiality

The Processor shall keep all Personal Data confidential and shall not disclose any Personal Data in any way to any Third Party without the prior written approval of the Controllers, except where, subject to this DPA, (i) such disclosure is required for the performance of the Deposit Agreement, this DPA or the Processing by a Sub-Processor, (ii) Personal Data need to be disclosed in relation to Clause 9 (*Audit*) of this DPA, or (iii) Personal Data need to be disclosed pursuant to applicable EU or EU Member State law. In case of such requirement of EU or EU Member State law, the Processor shall inform the Controllers of that legal requirement before Processing the Personal Data, unless that law prohibits such information to be provided to the Controllers on important grounds of public interest. If the Processor is required by law or requested to disclose Personal Data the Processor may refuse to disclose or refrain from disclosing it, if this is sensitive information which is subjected to a derivative privilege (*afgeleid verschoningsrecht*) based on the attorney-client or notary-client privilege (or any analogous privilege) applicable to lawyers, civil law notaries or similar professionals working for the Processor or any of the Processor's group companies.

4.2 Persons under Processor's authority

The Processor ensures that any person authorised to Process Personal Data on its behalf, including any employee, intern, officer, agent or contractor

of the Processor, has committed himself or herself to confidentiality and security of the Personal Data on the basis of a written agreement or as committed under statutory confidentiality obligations.

5. TECHNICAL AND ORGANISATIONAL MEASURES

5.1 Security measures

a. The Processor shall take all appropriate technical and organisational measures to secure the Personal Data which are or will be Processed by the Processor on behalf of the Controllers against the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data and complies with Data Protection by taking, amongst others, the security measures set out in its information security policy, as amended from time to time (the current version of which is attached hereto as Annex C (NautaDutilh Information Security Policy)). The Processor will use reasonable efforts to ensure an appropriate level of security, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the Processing as well as the risk of varying likelihood and severity for the rights and freedoms of the Data Subjects. The measures shall also aim at preventing unnecessary collection and further Processing of Personal Data.

b. The Processor shall comply with any security requirements expressly required by the Controllers, to the extent reasonably necessary to comply with Data Protection Laws.

c. In order to maintain an appropriate level of security as described in paragraph a. above, the Processor shall perform regular security checks and implement updates where required.

5.2 Data Subject Rights

a. Taking into account the nature of the Processing, the Processor shall provide the Controllers with all reasonably necessary assistance by appropriate technical and organisational measures, including (the implementation of) appropriate procedures and associated measures, insofar as this is reasonably possible, for the fulfilment of the Controllers' obligation to respond to requests for exercising any Data Subject Rights. This includes, taking into account the nature of the

Processing, measures allowing the Processor to access, rectify, erase or restrict Personal Data or providing Personal Data to the Controllers in a structured, commonly used and machine-readable format.

b. The Processor shall re-direct any request from a Data Subject to exercise any of its Data Subject Rights to the Controllers.

6. SUB-PROCESSORS

6.1 Controllers' authorisation

a. The Processor is allowed to permit Sub-Processors to Processing Personal Data under this DPA. This Clause constitutes a general written authorisation in accordance with the GDPR. The Processor will inform the Controllers prior to having Personal Data Processed by a new Sub-Processor. The Controllers can always oppose to the use of a specific Sub-Processor if it demonstrates that such Sub-Processor cannot ensure the adequate protection of the Personal Data.

b. The Processor shall remain fully and unconditionally liable to the Controllers for the Sub-Processor's performance of any obligation or part of it arising out of the Deposit Agreement, this DPA or any other agreement between the Controllers and the Processor.

c. The Controllers are deemed to have authorised in writing the Processing of Personal Data by the Sub-Processors engaged by the Processor at the date hereof. The Processor shall notify the Controllers of any intended changes concerning the addition or replacement of other Sub-Processors, thereby giving the Controllers the opportunity to object to such changes. If, within 10 Business Days of receipt of this notice, the Controllers have not objected to the intended change, the Controllers are deemed to have authorised the intended change.

6.2 Contract with Sub-Processor

The Processor shall impose on all Sub-Processors written data protection obligations that offer at least the same protection of Personal Data as the data protection obligations to which the Processor is bound on the basis of the Deposit Agreement and this DPA.

7. PERSONAL DATA BREACHES AND DPIAS

7.1 Personal Data Breaches

a. The Processor shall inform the Controllers of any Personal Data Breach without undue delay and in any case within thirty-six (36) hours after becoming aware thereof by e-mail to Datalekken_qct@aegon.nl.
b. In the event of a Personal Data Breach, the Processor shall promptly take all adequate remedial measures to end the Personal Data Breach and to mitigate any possible damages.
c. The information under paragraph a. above should include all information the Processor has in relation to the Personal Data Breach, allowing the Controllers to comply with its notification obligations under Data Protection Laws (where applicable) and the name of the Processor's data protection officer.
d. The Processor shall supplement its notification to the Controllers without undue delay with any additional information it obtains about the Personal Data Breach.
e. The Processor shall promptly provide the Controllers with any further information as reasonably requested by the Controllers regarding the Personal Data Breach.
f. The Processor shall cooperate with the Controllers to investigate the nature and scope of the Personal Data Breach and provide any other assistance as reasonably required by the Controllers to allow the Controllers to comply with any of its legal obligations, including notification obligations, in this respect, taking into account the nature of the Processing and the information available to the Processor.

7.2 DPIAs and Prior Consultations

Taking into account the nature of the Processing and the information available to the Processor, the Processor shall, upon the Controllers' reasonable request, assist the Controllers with ensuring compliance with any of Controllers' obligations under Data Protection Laws, in relation to DPIAs and prior consultation of a Supervisory Authority.

8. DELETION OR RETURN

8.1 Obligation to delete or return Personal Data

Upon termination of the Deposit Agreement or at the written request of the Controllers, the Processor shall, at the choice of the Controllers, return the Personal Data and all copies thereof to the Controllers and/or shall securely destroy (delete) such Personal Data and all existing copies thereof, except to the extent applicable EU or EU Member State statutory provisions require longer storage. In such case, the Processor shall inform the Controllers of such legal obligation, shall keep the Personal Data confidential and shall only Process the Personal Data to the extent required by the applicable EU or Member State law.

8.2 Deletion or return term

Any request of deletion or return of Personal Data under this Clause shall be performed by the Processor within a reasonable period after the date of the request from the Controllers or termination of the Deposit Agreement. The Controllers may require the Processor to confirm in writing that the Processor has returned or destroyed all Personal Data and copies thereof in accordance with the request of the Controllers.

9. AUDIT

The Controllers is entitled to request the Processor to verify its compliance with this DPA, or have this verified by an external third party (auditor) mandated by the Processor (on the Controllers' behalf), including in relation to any security measures taken by the Processor. The Processor shall make available all information necessary to demonstrate its compliance with the obligations laid down in this DPA. The Controllers shall bear the costs related to the verification of the Processor's compliance with this DPA within the meaning of this Clause.

10. TRANSFER/ACCESS OUTSIDE OF THE EEA

10.1 Transfers to Non-EEA Recipients

The Processor shall not transfer, which includes granting access to, Personal Data to a Non-EEA Recipient, unless:

a. an Adequacy Decision exists in relation to the Non-EEA Recipient. The Processor shall inform the Controllers of any such transfer of Personal Data and about the existence of the Adequacy Decision;
b. the transfer of Personal Data is ensured through application of an Appropriate Safeguard. In light hereof, the Controllers hereby mandate the Processor to enter into data transfer agreements with Non-EEA Recipients on the basis of EC Standard Contractual Clauses on its behalf, and approves the related transfers of Personal Data to Non-EEA Recipients; or
c. in the absence of an Adequacy Decision or Appropriate Safeguard, the conditions set forth in Article 49 GDPR, regarding derogations for specific situations, are met.

10.2 Adjustment of Appropriate Safeguards

Where any of the Appropriate Safeguards applying to a transfer under this Clause requires adjustment or is invalidated as a result of any change in Data Protection Laws or decision of a Supervisory Authority or other competent authority, the Parties shall ensure that the necessary adjustments to the EC Standard Contractual Clauses or Appropriate Safeguards are made or that the necessary alternative EC Standard Contractual Clauses or Appropriate Safeguards are implemented to ensure that the transfer(s) remain to be performed in compliance with Data Protection Laws.

11. LIABILITY

The Deposit Agreement governs the distribution of liability between the Parties.

12. TERM

The term of this DPA is the same as the term of the Deposit Agreement. Regardless of the termination of this DPA, the Processor is obliged to comply with the provisions of this DPA as long as Personal Data are Processed by Processor on behalf of Controllers. Clause 1 (*Definitions and Interpretation*), Clause 4 (*Non-Disclosure and Confidentiality*), Clause 12

(*Term*), Clause 13 (*Miscellaneous*) and Clause 14 (*Governing law and Jurisdiction*) shall survive indefinitely.

13. MISCELLANEOUS

13.1 Notices

The Processor shall inform the Controllers if it receives:

i. an inquiry, a subpoena or a request for inspection or audit from a competent authority or court relating to the Processing of Personal Data under the Deposit Agreement or this DPA, except where applicable law prohibits such information to be provided to the Controllers on important grounds of public interest;

ii. a subpoena or other request for disclosure of Personal Data Processed under the Deposit Agreement or this DPA to any competent authority, court or Third Party, except where applicable law prohibits such information to be provided to the Controllers on important grounds of public interest.

13.2 Precedence

a. Nothing in this DPA reduces the Parties' obligations under the Deposit Agreement or any other agreement between the Parties in relation to the protection of Personal Data or permits the Processor to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Deposit Agreement or any other agreement between the Parties.

b. In the event of inconsistencies between the provisions of this DPA and any other agreements between the Parties, including the Deposit Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the Parties) agreements entered into or purported to be entered into after the date of this DPA, the provisions of this DPA shall prevail.

13.3 Severance

Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure

its validity and enforceability, while preserving the Parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

13.4 Amendments

The Processor may amend this DPA if it deems such amendment reasonably necessary, at its sole discretion, to comply with Data Protection Laws, other applicable laws, rules and regulations or by change in the Personal Data Processed. Notwithstanding the foregoing, the Processor shall notify the Controllers of such changes in advance and enter into good faith negotiations with the Controllers on intended changes.

14. GOVERNING LAW AND JURISDICTION

a. This DPA shall be governed by the laws of the Netherlands (including the submission to jurisdiction pursuant to paragraph b. of this Clause).
b. The courts of Amsterdam, the Netherlands have exclusive jurisdiction to settle any dispute arising from or in connection with this DPA.

This DPA has been entered into on the date stated at the beginning of this DPA.

[*signature page follows*]

AGREED by the Parties' following authorised representatives

For and behalf of Controllers:

AEGON BANK N.V.

by :	by :
title :	title :

AEGON HYPOTHEKEN B.V.

by :	by :
title :	title :

AEGON LEVENSVERZEKERING N.V.

by :	by :
title :	title :

THE PROCESSOR
NAUTADUTILH N.V.

by :
title :

ANNEX A

DEFINITIONS

"**Adequacy Decision**"	means a decision of the European Commission in relation to a third country, a territory or one or more specified sectors within that third country, or an international organisation, within the meaning of Article 45 GDPR.
"**Annex**"	means an annex to this DPA.
"**Appropriate Safeguards**"	means appropriate safeguards within the meaning of Article 46 GDPR, including application of EC Standard Contractual Clauses or binding corporate rules within the meaning of Article 47 GDPR.
"**Clause**"	means a clause in this DPA.
"**Data Protection Laws**"	means all applicable laws (including EU and Member State laws), rules and regulations and sectoral recommendations relating to data protection and privacy with respect to the Processing of Personal Data, in each case including any amendments thereto or successors thereof, including the GDPR, national implementation laws relating to the GDPR (including the Dutch GDPR Implementation Act (*Uitvoeringswet AVG*)), Directive 2002/58/EC (as amended by Directive 2006/24/EC and Directive 2009/136/EC) and national implementation laws relating thereto (including the Dutch Telecommunications Act (*Telecommunicatiewet*)) and any security requirements as set out therein.
"**Data Subject**"	means any data subject (as defined in the GDPR) whose Personal Data are Processed

	by the Processor in the course of the performance of this DPA.
"**Data Subject Rights**"	means the rights of Data Subjects as set out in Chapter III of the GDPR.
"**Deposit Agreement**"	has the meaning given to this term in the recitals of this DPA.
"**DPA**"	means this Data Processing Agreement.
"**DPIA**"	means a data protection impact assessment within the meaning of Article 35 GDPR.
"**EC Standard Contractual Clauses**"	means standard data protection clauses as adopted by the European Commission, within the meaning of Article 46 GDPR.
"**EEA**"	means the European Economic Area.
"**GDPR**"	means Regulation (EU) 2016/679 of the European Parliament and 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.
"**Non-EEA Recipient**"	a party that is located in a third country within the meaning of the GDPR or an international organisation (as defined in the GDPR).
"**Party**"	means a party to this DPA.
"**Personal Data**"	means any personal data (as defined in the GDPR) which is Processed by the Processor on behalf of the Controllers in relation to the Services.
"**Personal Data Breach**"	means a personal data breach (as defined in

	the GDPR) with respect to Personal Data.
"**Processing**"	means processing (as defined in the GDPR).
"**Services**"	means the services provided by the Processor to the Controllers on the basis of the Deposit Agreement, as further described in Annex B (*Details of Processing*).
"**Supervisory Authority**"	means a supervisory authority as defined in the GDPR and any other supervisory authority competent in relation to the Processing of Personal Data under this DPA, including any consumer or telecommunications authority.
"**Sub-Processor**"	means any Third Party that is sub-contracted by the Processor to Process Personal Data on behalf of the Controllers, under the supervision of the Processor, but that does not fall under the direct authority of the Processor, at the date of this DPA being Koninklijke KPN N.V., Microsoft and Sentia Group B.V.
"**Third Party**"	means any party other than the Parties to this DPA.

ANNEX B

DETAILS OF PROCESSING

Nature of the Processing

The Processor will process the Personal Data as required for the provision of the Services. This includes:

- filing the Escrow Lists of Loans in accordance with clause 2.2 of the Deposit Agreement;
- replacing any Escrow List of Loans with an updated Escrow List of Loans (and therefore deleting the previous Escrow List of Loans) in accordance with clause 2.1 of the Deposit Agreement;
- releasing Escrow Lists of Loans to the Issuer and the Security Trustee subject to the fulfilment of the condition set forth in clause 3 of the Deposit Agreement;
- destroying Escrow Lists of Loans in accordance with clause 5.2 of the Deposit Agreement.

Types of Personal Data

Names (first name, last name), addresses (street, number, postal code, city) and loan number and, if different from the aforementioned address, the relevant address of the properties encumbered with a mortgage right.

Categories of Data Subjects

Debtors under the Relevant Mortgage Receivables, as listed on each Escrow List of Loans.

Purpose(s) of Processing

The performance of the Services under the Deposit Agreement.

Groups of employees of the Processors with access to the Personal Data

Members of the Processor's notarial department which are involved with the relevant matter relating to the Deposit Agreement, including the relevant (deputy) civil law notaries and the notarial support staff members.

ANNEX C

NautaDutilh – Information Security Policy 6.0 (ENG)

PREFACE

Every day, organisations are confronted with security risks. In addition to well-known tangible risks, the risk of information security breaches is growing: think for instance of the threat of computer viruses, failures of critical business systems, undesirable internet behaviour of employees or theft of laptops, smartphones and company data. Whether it concerns paper, computers or other telecommunications equipment, Information Security requires an increasing amount of attention from organisations.

Larger organisations usually pay attention to Information Security in a structured manner. Managers have often personally experienced the consequences of security risks. In addition, external supervisors are pointing out the various risks, based on relevant legislation or otherwise.

As the Board of NautaDutilh, we recognise the importance of Information Security, and we consider it our responsibility towards our clients to define how we addresses that. Information Security is part of our day-to-day responsibilities. We weigh up the efforts required (both in financial terms and in terms of the necessity for business operations) against the risks we run, as best as we can. NautaDutilh's Information Security Policy defines the general guidelines for NautaDutilh's approach to Information Security. The policy's details and guidelines containing functional and technical measures are contained in separate documents.

1 INTRODUCTION

Information and data form important information assets for NautaDutilh. Information assets that require serious considerations and assessments as far as protection against undesired influences is concerned. As a result of increasing integration of automated data processing and information provision in the primary processes, the importance of information assets has grown, and so has our dependence on them. Information assets also play an important role in delivering NautaDutilh's strategy.

1.1 Purpose of Information Security

The purpose of Information Security is to control the risks relating to the availability and continuity of information provision as well as the confidentiality and integrity of information. Management of these risks serves to support the

organisation's continuity, to limit risks and to maximise investment yields and opportunities.

The concrete Information Security measures are determined by performing a risk analysis in conjunction with NautaDutilh's strategy and objectives. Measures consist of policy, guidelines, procedures, working methods, organisational structures, and software and equipment functions. The system of measures should be balanced and consist of measures with different effects: preventative, detective, repressive and corrective.

Measures are determined, checked, assessed and where necessary improved in order to deliver NautaDutilh's specific security and organisational targets. It involves interaction with other management processes, such as risk management, compliance and audit.

In defining measures, NautaDutilh uses an internationally accepted and commonly used standard for information security: ISO 27002 (the code for information security).

Information Security is the concern of the entire organisation, headed by NautaDutilh's Board. The Board, the Information Security Committee and the Practice Group Managers have special roles in terms of policy determination and implementation of measures. Supervision of compliance is mainly the task of external and internal auditors.

1.2 Definition

NautaDutilh uses the following definition for Information Security:

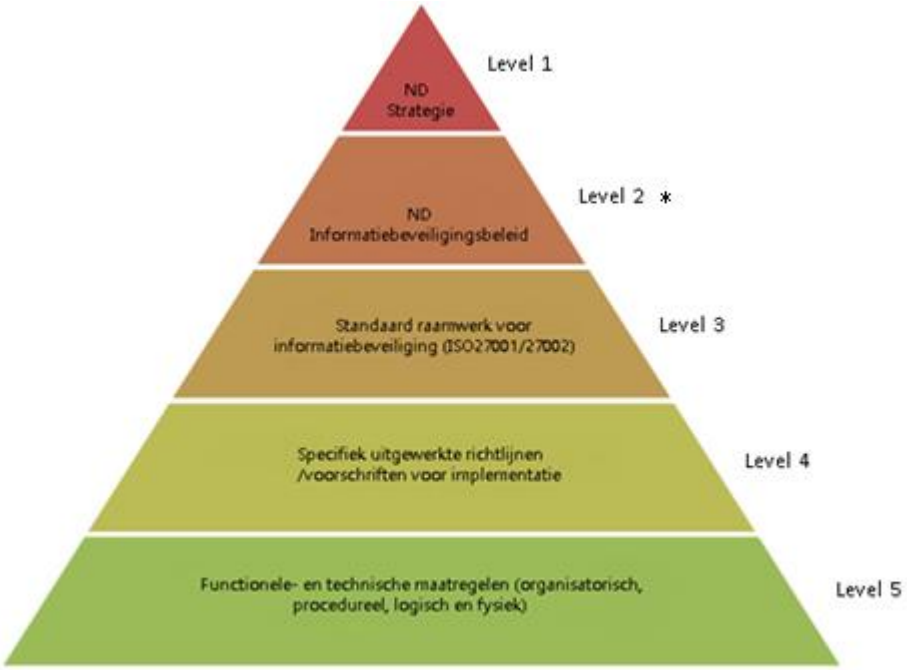
"The development and maintenance of a comprehensive system of measures to protect confidentiality and integrity of information as well as the continuity and availability of information provision".

1.3 Structure of Information Security Policy

The Information Security Policy represents the strategic view of NautaDutilh's Board on Information Security and on the application of information risk management.

The figure below reflects the different levels of the entire Information Security Policy. The Information Security Policy is formulated at top level (as set out in this document), on the basis of NautaDutilh's strategy, which includes "delivering quality and comprehensive legal services and solutions" and the core words fast, careful and decisive. At lower levels, the policy is developed into guidelines and

finally, into concrete measures. Each level controls the level below it.



* This document describes level 2.
[Translation of the figure: Level 1: ND Strategy / Level 2: ND Information Security Policy / Level 3: Standard framework for information security (ISO 27001/27002) / Level 4: Specific guidelines/implementation rules / Level 5: Functional and technical measures (organisational, procedural, logical and physical)]

1.4 Purpose of this document

The purpose of this document is to indicate the policy principles for Information Security at the highest level.

1.5 Legal framework

The use and development of the internationally accepted standard for information security (ISO 27001/27002) means that NautaDutilh also complies with information security requirements laid down in applicable laws, legislation and guidelines that apply to it.

1.6 Scope

1.6.1 Environment

The Information Security Policy forms part of NautaDutilh's general security policy, and is aimed at:

- All threats, internal or external, direct or indirect, deliberate or unintentional, aimed at all material or immaterial information assets of NautaDutilh, both at centralised and decentralised level;
- All media on or through which data is generated, processed, stored and distributed;
- All employees;
- All suppliers.

1.6.2 Starting points

In determining the Information Security Policy, the starting point is to limit the risks which NautaDutilh runs in its information provision by:

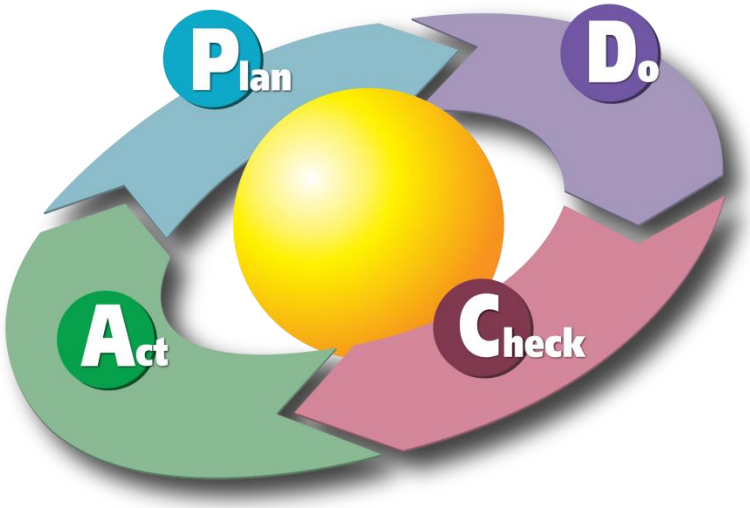
- Creating awareness in the organisation on the use of information, ICT resources and ICT information systems;
- Taking proper measures of an organisational, logical and physical nature;
- Discovering and reporting Information Security incidents in good time;
- Limiting the damage caused;
- Restoring to the original condition;
- Making the data owner primarily responsible for its data;
- Classifying data;
- Restricting a person's access to information to data that is absolutely necessary for the performance of that person's job;
- Ensuring all employees comply with the Information Security Policy.

1.7 Process-based approach to Information Security

The information security code lays down that Information Security must be implemented in terms of processes through an Information Security Management System (ISMS). NEN-ISO/IEC 27001:2013 offers a model to determine, implement, perform, check, assess, maintain and improve the ISMS. A PDCA model (Plan, Do, Check, Act model) is applied for this purpose. NEN-ISO/IEC does not describe an ISMS, but contains standards the ISMS should comply with. This Information Security Policy focuses entirely on NEN-ISO/IEC 27001:2013. The ISMS is described separately and maintained by the Security Manager.

A process-based approach to Information Security results in many double

qualitative guarantees. Implementation of Information Security in line with the process steps set out below will result in a controlled and effective implementation of Information Security measures.



1.8 Document characteristics

1.8.1 Revisions

Date	Author	Version	Changes
16-01-2015	D. Langhorst	0.1	First draft
04-02-2015	D. Langhorst	0.2	Processing ISO27001/ISO27002 best-practices
16-02-2015	D. Langhorst	0.3	Processing input from Fox-IT
23-03-2015	D. Langhorst	0.4	Processing input from Jeannette Wiers, Jurian Hermeler and Marc Weersink
08-04-2015	D. Langhorst	0.9	Changes from Information Security Committee
14-04-2015	D. Langhorst	1.0	1.0 NL & ENG version
22-10-2015	D.Langhorst	1.1	Update ISO/IEC27001:2005

			to ISO/IEC27001:2013
12-07-2016	D.Langhorst	2.0	Revised document based on changes to the security organization, policy framework and Information Handling.
22-08-2017	D.Langhorst	3.0	Revised document based on changes to the security organization, policy framework and Information Handling.
21-06-2018	D.Langhorst	3.1	Minor changes after yearly review
14-01-2019	D.Langhorst	4.0	Board members update and additional security measures
04-02-2020	D.Langhorst	5.0	Changes to the Security Organisation
15-02-2021	D.Langhorst	6.0	Added link to ND DPMF

1.8.2 Signatures

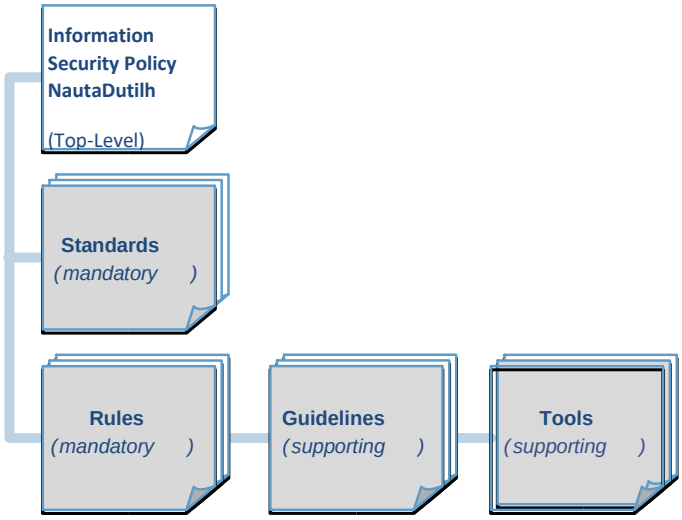
Name	Position	Date	Signatures
Petra Zijp	Board of NautaDutilh		
Chris Warner	Board of NautaDutilh		
Jaap Jan Trommel	Board of NautaDutilh		

2 STRUCTURE OF THIS DOCUMENT

The high-level Information Security Policy is described in sections 4 to 14 in line with the outline of ISO 27002, the international standard for information security. This represents level 3 "Standard framework for Information Security" in the security pyramid of section 1.3 on page 4.

2.1 Structure of the NautaDutilh Security Policies(NDSP)

The NDSP consists of this Information Security Policy NautaDutilh and an underlying set of documents (“framework”). The framework contains requirements for implementing the base security, continuity and privacy measures.



(NautaDutilh Security Policy(NDSP) Structure)

Standards contain statements on WHAT needs to be in place (requirements) and WHY (rationale). Standards are primarily aimed at management. Requirements in a standard contain limited details on how measures must be implemented.

Rules which are mandatory describe in a practical manner HOW certain measures must be implemented. Rules are aimed at developers, architects, administrators, asset owners, security professionals, corporate departments, shared service centres, etc.

Guidelines and Tools are not mandatory per se, unless a guideline or tool is referred to in a standard or rule document and is declared mandatory. Guidelines and Tools provide guidance on implementation of measures.

The structure of the NDSP is explained in more detail in the Security and Continuity Management Standard (NDSP-FA01-ST01).

3 RISK ASSESSMENT AND RISK MANAGEMENT

Risk management can identify a need to secure information assets. After analysis, this need can be translated into policy, guidelines and measures (levels 4 and 5). Furthermore, the Information Security Policy is created on the basis of risk analysis and there will have to be optimum alignment with the starting points and working methods used.

4 SECURITY POLICY

4.1 Information Security Policy

1. The Information Security Policy is a leading factor in the approach to Information Security at NautaDutilh, in accordance with the organisational requirements and applicable laws and legislation. The Information Security Policy forms part of NautaDutilh's Information Security Management System (ISMS).
2. The Executive Board is responsible for NautaDutilh's Information Security.
3. The members of the Data Protection Management Team are responsible for ensuring that the various business units within NautaDutilh implement and comply with the Information Security Policy.
4. The Practice Group Managers ensure that their practice group implements and complies with the Information Security Policy.
5. The Practice Group Managers are responsible for the security of information within the practice group.
6. The directors ensure that staff departments implement and comply with the Information Security Policy.
7. The directors are responsible for the security of information within the staff departments.
8. The CISO is responsible for drawing up and maintaining the Information Security Policy.
9. The Data Protection Management Team advise and support the CISO when drawing up and maintaining the Information Security Policy.
10. External and internal auditors supervise the setup, the existence and the operation of the Information Security Policy and the functioning of the Information Security organisation.

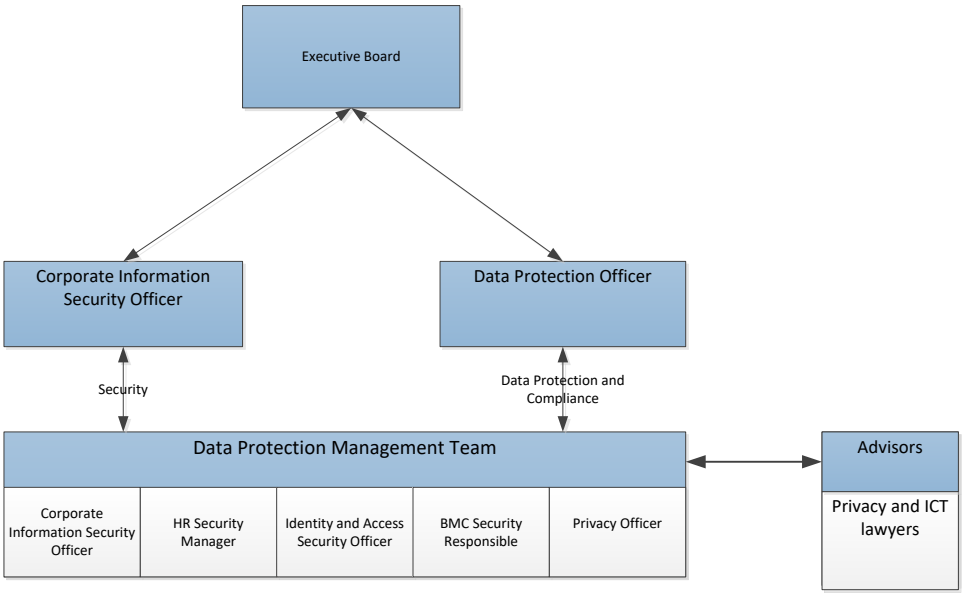


Figure 1. High Level Information Security Organisation

5 ORGANISATION OF INFORMATION SECURITY

5.1 Internal organisation

1. NautaDutilh uses a management framework to initiate, coordinate and control implementation of Information Security within the organisation. (Link to Data Protection Management Framework)

ND Data Protection Management Framew

2. The Board allocates security roles and security responsibilities.
3. The Board ensures that the means are available for ensuring a sufficient Information Security level.
4. Delegation of security responsibilities is allowed. Responsibilities may not be transferred.
5. Employees and third parties will work together and assist one another in the field of Information Security.
6. Employees and third parties know and commit to NautaDutilh's Information Security Policy.
7. NautaDutilh maintains its knowledge in the field of Information Security.

5.2 External parties

1. When introducing products or services from external parties, the security of NautaDutilh's information assets is maintained.
2. By way of a risk analysis, NautaDutilh determines the security implications and the control measures to be implemented when external parties are deployed.
3. NautaDutilh lays down the control measures and responsibility in an agreement with the external party. This agreement is signed before the work commences.

6 INFORMATION ASSETS MANAGEMENT

6.1 Responsibility for information assets

1. NautaDutilh documents the importance of information assets and keeps this information updated.
2. Information assets have an "owner".
3. Information assets that are processed commercially are and remain the legal property of NautaDutilh.
4. The owner is responsible for regular classification of information assets and supervises the correct application of Information Security measures.
5. NautaDutilh documents and implements rules for acceptable use of information assets.

6.2 Classification of information

1. Information must be classified in order to indicate the expected level of protection when it is handled.
2. Information at NautaDutilh must be classified at least as confidential.

7 HUMAN RESOURCES SECURITY

7.1 Prior to employment

1. Security responsibilities are laid down in proper job descriptions and in the employment conditions.
2. NautaDutilh screens its employees in accordance with the guidelines for each job profile.
3. Employees accept and sign the conditions of their employment contract, in which NautaDutilh lays down the employee's responsibilities and those of the organisation with respect to Information Security.

4. Employees and third parties sign a confidentiality agreement from NautaDutilh prior to commencing the work.

7.2 During employment

1. Employees apply security in accordance with the determined policy and procedures.
2. Employees have a proper level of awareness, education and training in security procedures and the correct use of ICT facilities in order to minimise any security risks. NautaDutilh determines a formal process on how to deal with security breaches.
3. Managers pay attention to Information Security during the appraisal interviews.

7.3 Termination of employment or change in employment

1. Employees who leave the organisation must hand in all equipment and other means made available to them. NautaDutilh withdraws all access rights. Knowledge that is important for ongoing operations is documented and transferred to the organisation.
2. If an employee is suspended, NautaDutilh withdraws the access rights of that employee.
3. NautaDutilh treats changes in responsibilities and the employment contract within the organisation as termination of the responsibility or relevant employment in question. The taking up of the new responsibilities or new job is then considered as entering into a new employment contract.

8 PHYSICAL AND ENVIRONMENTAL SECURITY

8.1 Secure areas

1. Information assets supporting critical or sensitive organisational activities are physically placed in secure areas in accordance with ISO 27002.
2. Information assets are physically protected from access by unauthorised persons, damage and malfunctions.
3. Offices, secure and other areas and facilities are physically protected from unauthorised access and unauthorised disclosure of information assets, in line with their classification.
4. NautaDutilh places the most important information assets in areas that third parties (non-NautaDutilh employees) cannot access.

8.2 Security of equipment

1. NautaDutilh places, protects, maintains and controls all information assets, power cables and communications cables in such a way as to limit the risks of damage, external interruption and unauthorised access.
2. The risks of working with information assets outside of NautaDutilh's buildings are properly controlled in order to prevent security breaches of information assets.
3. Media storing information assets that are no longer required are destroyed or overwritten in a secure manner.

9 MANAGEMENT OF COMMUNCATIONS AND OPERATIONAL PROCESSES

9.1 Operational procedures and responsibilities

1. NautaDutilh guarantees a correct and safe operation of information assets.
2. NautaDutilh controls the risk of negligence or intentional abuse of information assets.
3. NautaDutilh controls changes in information assets with strict change management.
4. NautaDutilh maintains a strict division between facilities for development, test, acceptance and production within the automated processing environment.

9.2 Supplier relationship management

1. NautaDutilh applies and maintains a suitable level of Information Security and service provision in the agreements for services provided by third parties.
2. NautaDutilh manages changes in the service provision by third parties, taking into account the quality requirements for information assets and operational processes, and reconsiders risks.
3. NautaDutilh checks and regularly assesses the services, reports and registrations performed by third parties, and regularly performs audits.
4. The third party ensures compliance with implementation and maintenance of the agreed security requirements and security measures.

9.3 System planning and system acceptance

1. NautaDutilh takes measures to guarantee sufficient capacity and availability of resources necessary to deliver the required system performance and to limit the risk of system disruptions.
2. NautaDutilh determines acceptance criteria for new information systems, upgrades and new versions, and carries out appropriate system tests during development and prior to acceptance.

9.4 Protection from malware

1. NautaDutilh takes measures to prevent and discover the introduction of malware.
2. NautaDutilh records all reports of the introduction of malware or attempts to introduce malware and properly follows up these reports.

9.5 Back-up

1. NautaDutilh creates back-up copies of information assets and regularly tests these in accordance with the defined back-up policy that is determined on the basis of data classification and risk analysis.

9.6 Network security management

1. NautaDutilh manages and controls its networks and properly protects them against threats and maintains security for the information assets that use the network, including information assets that are transmitted.

9.7 Handling of information assets

1. Information assets are protected against unauthorised publication, changes, removal and destruction.
2. NautaDutilh deletes information assets in a safe and secure manner if they are no longer required.

9.8 Exchange of information assets

1. NautaDutilh secures information assets that are exchanged within the organisation, within applications, between people (including orally) and with external entities, in line with the highest classification of the information that is exchanged.
2. Employees do not conduct confidential conversations in public places or open office environments, guest areas and meeting locations. Communications devices comply with all applicable laws and legislation.
3. NautaDutilh protects information assets that play a role in online transactions to prevent incomplete transmission, misrouting, unauthorised message alteration, unauthorised publication, unauthorised duplication or display of messages.
4. The reliability of the information assets available on a publicly accessible system is properly protected to prevent unauthorised disclosure or modification.

9.9 Monitoring and logging

1. Employees' transactions and activities on automated systems are at all times traceable to the person unless there is a strong justification for not doing so.
2. Information Security exceptions must be accompanied by a documented risk analysis and can only by allowed with the explicit acceptance of NautaDutilh's Security Manager.
3. NautaDutilh secures saved log data against breaches and unauthorised access and complies with laws and legislation when recording this data and granting inspection of it.
4. NautaDutilh monitors and checks whether the system use complies with the Information Security Policy.
5. NautaDutilh guarantees the homogeneity of log data over time.

10 ACCESS SECURITY

10.1 Access control requirements

1. NautaDutilh controls the access to information assets and processes based on organisational needs and security requirements. The rules for access security take note of policy on information distribution and authorisation.

10.2 User access management

1. NautaDutilh uses formal HR procedures for the employment contracts of employees.
2. NautaDutilh pays attention to granting, withdrawing (including temporary withdrawing) and regularly assessing access rights to all information assets and services.
3. The allocation and use of special authorisation is restricted and managed specifically.
4. The allocation of passwords is controlled by a formal process.

10.3 User responsibilities

1. Users are aware of their responsibility to maintain proper access security, especially with respect to the use of user Ids, passwords and security of ICT devices.
2. NautaDutilh has a clean desk policy for information assets.

10.4 Access control for networks

1. NautaDutilh controls access to both internal and external networks.
2. NautaDutilh automatically identifies equipment to authenticate connections from specific locations and equipment.

3. Groups of information services, employees and information systems are separated on networks.

10.5 Access security for operating systems

1. NautaDutilh protects access to operating systems in order to guarantee the integrity, availability and confidentiality of information assets.
2. NautaDutilh uses emergency procedures for emergencies.
3. NautaDutilh uses proper systems for password management.
4. The use of auxiliary software with which system and application control measures could be bypassed is restricted and strictly controlled.
5. Inactive sessions are blocked or automatically switched off after a certain period of inactivity.
6. Access to high-risk information assets is restricted by pre-defined periods.

10.6 Access control for information systems and information

1. In the use of information assets, NautaDutilh uses segregation of control functions in line with the adopted access policy.
2. Information systems are equipped with an appropriate security level.

10.7 Laptops and remote access

1. The protection of laptops is in line with the classification guideline for information.
2. Remote access/VDI is allowed after permission from the direct manager.
3. Additional authentication is obligatory when using external connections before access is granted to NautaDutilh's systems.
4. The security measures for remote access are at a higher level than those of NautaDutilh's office location(s).

11 ACQUISITION, DEVELOPMENT AND MAINTENANCE OF INFORMATION SYSTEMS

11.1 Security requirements for information systems

1. The Information Security requirements are included in the requirements for new information systems or expansions of existing information systems, on the basis of a risk analysis. The requirements are justified, agreed and documented as part of the total business case for an information system.

11.2 Correct processing in information systems

1. Appropriate control measures are built into information systems, including applications developed by employees. These control measures include validation of input data, internal processing and output data.
2. Additional control measures may be required for information systems that process or have an influence on sensitive or critical information assets. Such additional control measures are drawn up on the basis of the security requirements and a risk assessment.
3. The authenticity and integrity of messages between information systems is protected in accordance with the classification.

11.3 Cryptographic control measures

1. Cryptographic security is applied to information assets with high confidentially and integrity requirements that could in part arise from relevant agreements, laws and rules.
2. In situations where disputes could arise as to whether or not an event or act took place, use must be made of a service that can prove the non-repudiation of the event or act (e.g. a digital signature of an electronic agreement or payment).
3. The management of cryptographic keys is of great importance for the efficient use of cryptographic techniques. A key control process has been set up for this purpose.

11.4 Security of system files

1. NautaDutilh controls access to system files and the program's source code.
2. Exposure of sensitive or critical data in test environments is strictly prohibited. Test data are carefully selected, protected and controlled.
3. The installation of software on production systems is strictly limited to the allocated functions within the ICT organisation.

11.5 Security in development and support processes

1. NautaDutilh controls the implementation of changes by way of formal procedures for change management.
2. NautaDutilh limits changes to standard software packages to changes that are necessary.
3. NautaDutilh prevents that occasions occur that could lead to leaking of information assets.
4. Software development outsourced by NautaDutilh is supervised by NautaDutilh.
5. NautaDutilh takes contractual measures to protect the availability and maintenance of software specifically developed for the organisation in the event that the supplier is absent (escrow).

11.6 Technical vulnerability management

1. NautaDutilh implements the management of technical vulnerabilities in an efficient, systematic and repeatable manner, with measurements to confirm its efficiency.

12 INFORMATION SECURITY INCIDENT MANAGEMENT

12.1 Reporting Information Security incidents and weaknesses

1. NautaDutilh has formal procedures in place for reporting and escalating Information Security incidents.

12.2 Management of Information Security incidents and improvements

1. NautaDutilh has responsibilities and procedures in place for efficiently managing Information Security incidents and weaknesses.

13 BUSINESS CONTINUITY MANAGEMENT

13.1 Information Security aspects of business continuity management

1. NautaDutilh implements a process of business continuity management to reduce to an acceptable level the impact on the organisation caused by the non-availability of information assets (as a result of, for instance, natural disasters, accidents, equipment failure and intentional acts) and the recovery thereof.
2. NautaDutilh regularly tests and updates the business continuity process.

14 COMPLIANCE

14.1 Compliance with legal requirements

1. NautaDutilh explicitly defines all current legal and regulatory requirements and contractual obligations, updates them and guarantees that they are complied with.
2. Intellectual property rights are respected and protected at all times.
3. NautaDutilh protects important registrations against loss, destruction, falsification and unauthorised disclosure.
4. Information assets may only be used for the purposes defined to that end.

14.2 Compliance with security policies and standards and technical compliance

1. The security of information systems is regularly assessed against the security policy.
2. NautaDutilh assesses information systems in terms of compliance with applicable standards for the implementation of security and documented security measures.
3. The Security Manager regularly reports to the Board on compliance with the Information Security Policy.

14.3 Information systems audit considerations

1. Audits and other control activities of operational processes require planning and approval to reduce the risk of disruptions to operational processes to a minimum.
2. Tools for audits of information systems are properly protected against abuse or compromise.
3. Audits can and may only take place after formal approval of both the Security Manager and NautaDutilh's Board.