stratech

Contact
Pantheon 15
7521 PR Enschede

053 480 40 80
info@stratech.nl
stratech.nl

DATE	VERSION	SUBJECT
01-04-2025	1/2025	Stratech Shipment Privacy Conditions

Article 1. Applicability

1. These Stratech Shipment Privacy Conditions, in addition to the Stratech Shipment General Terms and Conditions and any other conditions, apply to all offers and agreements of Stratech Holding bv, with its registered office at Pantheon 15 in Enschede, the Netherlands, and to all operating companies of Stratech Holding bv, hereinafter jointly referred to as Stratech.
2. If provisions relating to personal data/privacy relating to offers and agreements or other applicable conditions are contrary to the provisions of these Stratech Shipment Privacy Conditions, the provisions of these Stratech Shipment Privacy Conditions prevail.

Article 2. Definitions

The following definitions apply in these Stratech Shipment Privacy Conditions:

- Personal Data: ‘personal data’ as referred to in the General Data Protection Regulation (GDPR) and described in appendix 1;
- Controller: the controller as referred to in the GDPR, being the client who has instructed Stratech to perform activities;
- Processor: the processor as referred to in the GDPR, being Stratech;
- Activities: all activities the client has instructed Stratech to carry out or that are performed or that are to be performed by Stratech on a different basis. The foregoing applies in the broadest sense of the word and, in any event, includes the activities arising from the agreement.

Article 3. General

1. The Stratech Shipment Privacy Conditions apply to all personal data that are processed by Stratech for the client within the context of the performance of the agreement, and to all other activities performed for the client and the personal data to be processed in that connection.
2. When performing work, the processor processes certain personal data for the controller.
3. The Stratech Shipment Privacy Conditions constitute an agreement or other legal act as referred to in article 28, paragraph 3 of the GDPR.
4. If the processor, on the basis of the Stratech Shipment Privacy Conditions, charges the controller any costs, these charges will be in accordance with the conditions and rates of the processor applicable at that time.

Article 4. Scope

1. By giving the instruction to perform work, the controller instructs the processor to process personal data on behalf of the controller, in the manner as set out in appendix 1, in accordance with the provisions of the Stratech Shipment Privacy Conditions and article 30, paragraph 2(b) of the GDPR.
2. The processor processes the personal data in accordance with the Stratech Shipment Privacy Conditions. The processor confirms that it will not process the personal data for other purposes.
3. Control of the personal data will never rest with the processor.
4. The processor only processes the personal data within the European Economic Area.

Article 5. Obligations of the controller

1. The controller must take the necessary measures to ensure that the personal data, given the purposes for which they are collected or subsequently processed, are correct and accurate and made available as such to the processor. The controller guarantees towards the processor that no more personal data are collected than is strictly necessary for the performance of the work.

Without prejudice to the obligations of the processor arising from these Stratech Shipment Privacy Conditions and the GDPR, the controller is responsible for the processing of the personal data as described in annex 1, as well as for fulfilment of the obligations which the client, in his/her capacity of controller, is subject to on the basis of the GDPR and related laws and regulations. The controller is responsible for all obligations he/she is subject to under the GDPR. More in particular, the controller must comply with the provisions of articles 24 and 25 of the GDPR by taking measures that include but are not limited to technical and organisational measures to ensure and to be able to demonstrate that the processing is in accordance with the GDPR (article 24, paragraph 1 of the GDPR), taking into account the nature, scope, context and purpose of the processing, as well as the various risks to the rights and freedoms of natural persons in terms of the probability and severity thereof.

2. Furthermore, the controller, taking into account the state of the art, the implementation costs and the nature, scope, context and purpose of the processing, as well as the various risks to the rights and freedoms of natural persons in terms of the probability and severity thereof in relation to the processing, both when determining the means of processing and during the processing itself, will implement appropriate technical and organisational measures, such as pseudonymisation, which have been designed to effectively implement data protection principles such as data minimisation and to integrate the necessary safeguards into the processing, in order to comply with GDPR regulations and protect the rights of data subjects (article 25, paragraph 1 of the GDPR). The controller will further implement appropriate technical and organisational measures, thereby ensuring that in principle only personal data are processed that are necessary for each specific purpose of processing (article 25, paragraph 2 of the GDPR).
3. The data controller will forward the name and contact details and, if appointed, the details of the data protection officer as referred to in article 30, paragraph 2(a) of the GDPR, to the processor and notify him/her of any changes therein.
4. The controller guarantees that it shall not require the processor to process personal data whereby personal data are transferred to any third country or international organisation as referred to in article 30, paragraph 2(c) of the GDPR.
5. The controller indemnifies the processor against possible claims from third parties, including but not limited to those of data subjects as referred to in the GDPR and those of the Dutch Data Protection Authority, in connection with the breach of obligations of the controller pursuant to the provisions in this article and the GDPR.

Article 6. Confidentiality

1. The processor and the persons employed by the processor or who perform work for him/her, insofar as these persons have access to personal data, only process the personal data on behalf of the controller, subject to deviating legal obligations or a court ruling to the contrary.
2. The processor and the persons employed by the processor or who perform work for him/her, insofar as these persons have access to personal data, are obliged to keep the personal data which they become aware of secret, except insofar as any legal requirement or court ruling obliges them to disclose or the requirement to disclose arises from a task. The obligation as referred to in the previous sentence applies both during the term of the agreement(s) with the controller and afterwards.

Article 7. No further provision

1. The processor will refrain from sharing personal data with third parties or otherwise making these available to them unless the processor has been given prior written approval or an instruction from the controller to do so or is otherwise obliged to do so by virtue of the laws and regulations or a court ruling.

2. If, by virtue of the laws and regulations, the processor is obliged to share the personal data with third parties or otherwise make these available to them, the processor must notify the controller thereof in writing unless this is not permitted under said laws and regulations or court ruling.

Article 8. Security measures

1. The processor, taking into account the applicable laws and regulations concerning the security of the processing of personal data, the state of the art, the implementation costs and the nature, scope, context and purpose of processing, as well as the various risks to the rights and freedoms of natural persons in terms of the probability and severity thereof in relation to the processing, will take technical and organisational security measures to ensure a level of security appropriate for the risk and protect the personal data processed by the processor against infringements in connection with the personal data as referred to in article 4(12) of the GDPR. The measures are partly aimed at preventing the collection and further processing of personal data beyond what is strictly necessary for the performance of the work. In those instances where article 4(12) of the GDPR refers to forwarded personal data, the responsibility of the processor only pertains to personal data received by him/her within the framework of an agreed assignment and which have been forwarded to him/her and not to personal data forwarded by the processor to the controller and/or third parties, other than sub-processor(s).
2. The security measures currently in place and of which the parties have determined that they are deemed appropriate as referred to in article 32, paragraph 1 of the GDPR, are set out in appendix 2 and at the same time serve as a description as referred to in article 30, paragraph 2(d) of the GDPR.

Article 9. Monitoring compliance

1. Within the framework of monitoring compliance by the processor with the Stratech Shipment Privacy Conditions, solely with regard to the security measures taken within that context as referred to in article 8, the processor, in accordance with the provisions of article 28, paragraph 3(h) of the GDPR, will have an audit carried out as part the Information Security Management System standard NEN-EN-ISO/IEC 27001:2023/A1:2024, the scope of which concerns at least the security measures referred to in Article 8.
2. The audits referred to article 28, paragraph 3(h) of the GDPR, including inspections, will not be carried out by the controller him/herself. In accordance with the provisions of the aforesaid article, the controller authorises the processor to appoint an auditor (the external expert referred to in paragraph 1) on behalf of the controller, in order to check compliance as referred to in paragraph 1.
3. The costs of the audit referred to in paragraph 1, are included in the costs of the subscription.
4. The costs of any other activities of the processor for monitoring compliance with the obligations under article 28, paragraph 3(h) of the GDPR, will be at the expense of the controller.

Article 10. Data breach

1. In accordance with the provisions in article 33, paragraph 2 of the GDPR, the processor notifies the controller without unreasonable delay as soon as he/she has taken note of a breach in relation to the personal data. The processor, insofar as possible, will provide information (as referred to in article 28, paragraph 3(f) of the GDPR) about the nature of the personal data breach, the probable consequences of the personal data breach and the measures taken and to be taken by the processor.
2. The provisions of paragraph 1 of this article do not affect the obligations of the controller under the GDPR in the event of infringements as referred to in paragraph 1, more in particular but not limited to the obligations under article 33 and 34 of the GDPR.

Article 11. Sub-processors

1. During the performance of the work under the Stratech Shipment Privacy Conditions, the processor is entitled to engage third parties (sub-processors, as referred to in appendix 1), for which the controller grants general permission as referred to in article 28, paragraph 2 of the GDPR. The processor notifies the controller of the intended changes in respect of the addition or replacement of sub-processors, whereby the controller is offered the opportunity to object to these changes. Objections must be received by the processor within ten days of the notification as referred to above, in the absence of which the controller is deemed not to object. In all cases, objections will not be submitted on unreasonable grounds. The controller is entitled to terminate the agreements with the processor which are subject to the intended change to which objection has been made, with immediate effect if the engagement of the relevant sub-processor means that continuation of such agreements within the context of the Stratech Shipment Privacy Conditions cannot reasonably be demanded from the controller. The processor is entitled to terminate the agreements with the controller which are subject to the intended change to which objection has been made, with immediate effect if without the engagement of the relevant sub-processors continuation of such agreements within the context of the Stratech Shipment Privacy Conditions cannot reasonably be demanded from the processor.
2. If the processor engages a sub-processor, the processor must impose the Stratech Shipment Privacy Conditions on the relevant sub-processor or, alternatively, the processor enters into a processor's or sub-processor's agreement with this sub-processor concerning the obligations of the sub-processor, in which the sub-processor is subject to the same data protection obligations as those imposed on the processor on the basis of the Stratech Shipment Privacy Conditions. If the sub-processor fails to comply with its obligations in respect of data protection, the processor remains fully responsible towards the controller for the performance of the obligations of said sub-processor.

Article 12. Liability

The processor is only liable for loss, insofar as this is caused by his/her activities as referred to in article 82, paragraph 2 of the GDPR, all this in accordance with the provisions of article 82, paragraph 2 of the GDPR. The processor is only liable for loss that is the direct and exclusive consequence of non-fulfilment of obligations by the processor under the Stratech Shipment Privacy Conditions.

Article 13. Cooperation in the event of requests for assistance

1. The processor, on the request of the controller, taking into account the nature of the processing and, insofar as this is possible, by taking appropriate technical and organisational measures, will assist the controller as referred to in article 28 paragraph 3(e) of the GDPR.
2. The processor, on the request of the controller, taking into account the nature of the processing and the information available to the processor, will assist the controller as referred to in article 28, paragraph 3(f) of the GDPR.
3. The processor is entitled to charge the costs he/she has to incur in connection with the provisions under paragraphs 1 and 2 to the controller.

Article 14. Term and termination

1. For as long as the processor performs activities for the controller, the Stratech Shipment Privacy Conditions will apply thereto.
2. If after the end of the agreement between the controller and the processor, the latter, under Union or Member State law, is obliged to store personal data during a statutory period, the processor will arrange for the removal of these personal data, one month after the end of the statutory retention obligation. The costs of complying with the statutory obligation to retain data can be passed on by the processor to the controller.
3. Upon termination of the agreement between the controller and the processor, the controller may request the processor, once and within one month of the end of the agreement, to provide the controller with the personal data available at the processor at the expense of the controller or to return it to him/her on a data carrier to be determined by the processor or by means of electronic transfer. The personal data will be erased after the end of the agreement, after the expiry of the aforesaid term of one month.

Article 15. Nullity

If one or more provisions of these Stratech Shipment Privacy Conditions are void or voided, the other conditions remain in full force. If any provision of these Stratech Shipment Privacy Conditions is void or voided, the parties will consult each other about the content of a new provision, which provision will reflect the content of the original provision as closely as possible.

Article 16. Changes to the Stratech Shipment Privacy Conditions

The processor has the right to change the Stratech Shipment Privacy Conditions, including the related appendix/appendices, unilaterally if this is reasonably appropriate in the opinion of the processor inter alia in connection with a change to legislation and regulations, case law pertaining to the GDPR and its interpretation, a change to the functionality of the online service, a change to the activities and/or the security measures and/or a change to the processor's policy. A change is effective from the moment the controller has received the amended Stratech Shipment Privacy Conditions.

These Stratech Shipment Privacy Conditions as well as the Dutch Privacy Voorwaarden Stratech Shipment were made available to the client prior to or at the time of the conclusion of the agreement to which these Stratech Shipment Privacy Conditions apply or after these Stratech Shipment Privacy Conditions were adopted. The conditions can also be read and can be downloaded from the Stratech website: www.stratech.nl.

These English Stratech Shipment Privacy Conditions are a translation of the Dutch Privacy Voorwaarden Stratech Shipment. If any provision of these English Stratech Shipment Privacy Conditions conflicts with the Dutch Privacy Voorwaarden Stratech Shipment, the provision of the Dutch Privacy Voorwaarden Stratech Shipment shall apply. The Dutch Privacy Voorwaarden Stratech Shipment have been filed with the Overijssel District Court, Almelo location, on 10/03/2023 under number 6/2023.

stratech

Contact
Pantheon 15
7521 PR Enschede

053 480 40 80
info@stratech.nl
stratech.nl

DATE	VERSION	SUBJECT
01-04-2025	1/2025	Stratech Shipment Privacy Conditions - Appendix 1

This appendix is Appendix 1 as referred to in the Stratech Shipment Privacy Conditions for controllers using the Stratech Shipment online service.

The controller instructs the processor to carry out work. As part of this work, personal data of persons may be processed. This appendix sets out what personal data are processed and the work the processor carries out in that context for the controller.

This appendix is in part subject to changes in the functionality of the online service and change as a result of an update for example.

1. Version management

DATE	CHANGE
12-06-2020	Version management added; Customs added to Interfacing functionality; In connection with the migration of the hosting environment from Root to Previder: ● management activities for the hosting environment by sub-processor Root deleted; ● sub-processor Previder added for management activities for the hosting environment.
06-10-2020	Removed Root sub-processor.
01-08-2022	Terminology aligned with the delivery conditions; Interfacing functionality adjusted; Analyses functionality added; Consultancy functionality added; Service provision functionality adjusted.
11-01-2023	Sub-processor Userlane GmbH added
01-04-2025	Updated address sub-processor Microsoft Corporation

2. Personal data[1]

The controller processes personal data which, separately or in combination, is likely to identify a natural person (identifying personal data). The controller uses Stratech's online service for this purpose. It relates to the (categories of) data set out below:

- User data
- Relation data

The controller will not record anything other than the (categories of) personal data referred to above.

[1] The possibility to process certain (categories of) personal data may depend on the configuration of the online service used by the controller.

3. Activities

The processor processes (categories of) personal data set out above for the controller. The activities follow from the agreements concluded between Stratech and the client and concern one or more of the following activities:

- Hosting;
  This refers to the management activities relating to the hosting whereby the personal data is included in the hosting environment of the processor.
- Interfacing;
  This concerns automated activities in the processor's hosting environment whereby personal data is exchanged (received or forwarded) through interfaces with the systems of third parties, such as the Chamber of Commerce, the Dutch Customs Administration (Customs) and ERP systems.
- Analyses;
  This largely concerns automated activities in which connection data, including personal data, are analysed for the purpose of obtaining anonymised statistical data, to improve and optimise the online service, to trace and fix errors and to support the client.
- Consultancy;
  This largely concerns activities that are performed by (a consultant of) the processor on location at the controller or from the location of the processor whereby the employee has (remote) access to the personal data.
- Service provision.
  This concerns activities carried out by (a service desk employee of) the processor, often at the location of the processor or, through remote access, from the location of the processor at the location of the controller, within the context of service reports concerning support relating to the online service and whereby the employee has (remote) access to the personal data.
  This concerns activities carried out by (an employee of) the processor, often at the location of the processor or, through remote access, from the location of the processor at the location of the controller, within the context of service reports concerning breakdowns and errors to the online service and whereby the employee has (remote) access to the personal data.

4. Sub-processors

The processor makes use of the following sub-processors to carry out activities.

Name: Previder BV
Contact details: Expolaan 50, 7556 BE in Hengelo
Activities: management activities for the processor's hosting environment.

Name: Microsoft Corporation
Contact details: One Microsoft Place, South County Business Park, Carmanhall And Leopardstown, Dublin, D18 P521, Ierland
Activities: management activities for the Microsoft Azure Core Services.

Name: Userlane GmbH
Contact details: Rosenheimerstraße 143C, D-81671 Munich, Duitsland
Activities: management activities for the Userlane Services.

stratech

Contact
Pantheon 15
7521 PR Enschede

053 480 40 80
info@stratech.nl
stratech.nl

DATE	VERSION	SUBJECT
01-04-2025	1/2025	Stratech Shipment Privacy Conditions - Appendix 2

This appendix is Appendix 2 as referred to in the Stratech Shipment Privacy Conditions for controllers using the Stratech online service referred to in appendix 1 (as referred to in the Stratech Shipment Privacy Conditions).

The controller instructs the processor to carry out work. As part of this work, personal data of persons may be processed. This appendix specifies the security measures taken by the processor.

1. Version management

DATE	CHANGE
03-05-2018	First version.
11-06-2019	Version management added; Update security measures.
14-08-2019	NEN certification removed from hosting provider.
11-03-2020	Tightened the measure relating to the allocation and use of special powers under ‘Access security’. In connection with the migration of the hosting environment from Root to Previder, changed the term ‘monthly’ into ‘on a regular basis’ under ‘Supplier relationships’.
27-11-2020	Language correction under “Employee-related security”, concerning the measure “As part of the terms of employment, employees must comply with their responsibilities related to information security”. Removal of the measures relating to: disaster recovery procedure, supplier control and changes to the supplier services.
18-05-2021	Overlapping security measures removed.
01-08-2022	Terminology aligned with the delivery conditions.
04-07-2023	Security measures adjusted due to NEN-EN-ISO/IEC 27001:2017+A11:2020 processor certification.
01-04-2025	Security measures adjusted due to NEN-EN-ISO/IEC 27001:2023/A1:2024 nl certification of processor.

2. Security measures

The processor processes personal data as referred to in appendix 1 for the controller. The activities arise from the agreements concluded between Stratech and the client. Processor works in accordance with a generally recognized standard for information security, namely NEN-EN-ISO/IEC 27001:2023/A1:2024 nl.

2.1. ISO certificate

DigiTrust
CERTIFICATION OF MANAGEMENT SYSTEMS

Management Systeem Certificaat

Dit certificaat met nummer DGT271721769 is uitgegeven voor het managementsysteem van:

Stratech Automatisering B.V.

Vestigingsadres: Pantheon 15, 7521PR te Enschede

Voldoet aan de eisen gesteld in de Informatie Beveiliging Management Systeem norm:

NEN-EN-ISO/IEC 27001:2023/A1:2024 nl

Voor het toepassingsgebied: Informatiebeveiliging gerelateerd aan het ontwikkelen van applicaties, het beschikbaar stellen van deze applicaties aan klanten via hosting, het ondersteunen van deze klanten bij het gebruik van de applicatie via service en consultancy, het adequaat beveiligen van de tot de applicatie behorende databank en de daarin opgeslagen (persoons)gegevens en ondersteunende processen voor veilig personeel en veilige voorzieningen.
Dit alles binnen de kaders van de met klant gesloten overeenkomst inclusief de van toepassing zijnde leveringsvoorwaarden en met uitsluiting van de eigen verantwoordelijkheid van een klant voor afdoende beveiliging van diens eigen systemen, gegevens (waaronder persoonsgegevens) en andere al dan niet gevoelige (bedrijfs)informatie.

In overeenstemming met de verklaring van toepasselijkheid versie 2.2 van 24 februari 2025.

Dit certificaat is alleen geldig in samenhang met het certificaataanhangsel met hetzelfde nummer, waarop de van toepassing zijnde locaties met betrekking tot dit certificaat vermeld zijn.

Dit certificaat is geldig vanaf:
4 maart 2025

Dit certificaat is geldig tot:
12 mei 2026

Datum eerste certificaat:
12 mei 2023

Dit certificaat vervangt nr:
DGT271721337

NAMENS

Marco Bijl
DigiTrust B.V.

RvA MGMT. SYS. C 618

DigiTrust B.V.: Achtseweg Zuid 159R - 5651 GW Eindhoven - Nederland
Telefoon +31 88 224-5600 - sales@digitrust.nl - www.digitrust.nl - KvK 59396822

Deze afgifte is uitgevoerd in overeenstemming met en binnen de procedures van DigiTrust zoals ook bekend bij en gecontroleerd door de RvA. Dit certificaat is elektronisch uitgegeven, het is en blijft eigendom van DigiTrust. Het valt daarom onder en is gebonden aan de uitgifte condities van het contract.
Certificaten kunnen worden gevalideerd via de QR-code.

Pagina 1 van 2

DigiTrust
CERTIFICATION OF MANAGEMENT SYSTEMS

Behorende bij het certificaat met registratienummer: DGT271721769
Het informatiebeveiligingsmanagementsysteem van: Stratech Automatisering B.V.

Werkmaatschappijen en geregistreerde activiteiten

Stratech Automatisering B.V.
Informatiebeveiliging gerelateerd aan het ontwikkelen van applicaties, het beschikbaar stellen van deze applicaties aan klanten via hosting, het ondersteunen van deze klanten bij het gebruik van de applicatie via service en consultancy, het adequaat beveiligen van de tot de applicatie behorende databank en de daarin opgeslagen (persoons)gegevens en ondersteunende processen voor veilig personeel en veilige voorzieningen.
Dit alles binnen de kaders van de met klant gesloten overeenkomst inclusief de van toepassing zijnde leveringsvoorwaarden en met uitsluiting van de eigen verantwoordelijkheid van een klant voor afdoende beveiliging van diens eigen systemen, gegevens (waaronder persoonsgegevens) en andere al dan niet gevoelige (bedrijfs)informatie.

Stratech Opleiding & Advies B.V.
Pantheon 15, 7521 PR Enschede

CERTIFICAAT

DigiTrust B.V.: Achtseweg Zuid 159R - 5651 GW Eindhoven - Nederland
Telefoon +31 88 224-5600 - sales@digitrust.nl - www.digitrust.nl - KvK 59396822
Deze afgifte is uitgevoerd in overeenstemming met en binnen de procedures van DigiTrust zoals ook bekend bij en gecontroleerd door de RvA. Dit certificaat is elektronisch uitgegeven, het is en blijft eigendom van DigiTrust. Het valt daarom onder en is gebonden aan de uitgifte condities van het contract.
Certificaten kunnen worden gevalideerd via de QR-code. Pagina 2 van 2

2.2. Declaration of Applicability (VVT)

ISO27001:2023/A1:2024(NL) VERKLARING VAN TOEPASSELIJKHEID STRATECH VERSIE 2.2 DATUM: 24-2-2025			VAN TOEPASSING?	GEÏMPLEMENTEERD?	VAN TOEPASSING VANUIT WET- EN REGELGEVING	VAN TOEPASSING VANUIT CONTRACT EN/OF SLA	RISICO ANALYSE	ONDERBOUWING WAAROM NIET VAN TOEPASSING
Nr.	**Onderwerp**	**Beheersmaatregel**						
5	**Organisatorische beheersmaatregelen**							
5.1	Beleidsregels voor informatiebeveiliging	Informatiebeveiligingsbeleid en onderwerp specifieke beleidsregels moeten worden gedefinieerd, goedgekeurd door het management, gepubliceerd, gecommuniceerd aan en erkend door relevant personeel en relevante belanghebbenden en met geplande tussenpozen en als zich significante wijzigingen voordoen, worden beoordeeld.	Ja	Ja		X	X	
5.2	Rollen en verantwoordelijkheden bij informatiebeveiliging	Rollen en verantwoordelijkheden bij informatiebeveiliging moeten worden gedefinieerd en toegewezen overeenkomstig de behoeften van de organisatie.	Ja	Ja		X	X	
5.3	Functiescheiding	Conflicterende taken en conflicterende verantwoordelijkheden moeten worden gescheiden.	Ja	Ja			X	
5.4	Management-verantwoordelijkheden	Het management moet van al het personeel eisen dat ze informatiebeveiliging toepassen overeenkomstig het vastgestelde informatiebeveiligingsbeleid, de onderwerpspecifieke beleidsregels en procedures van de organisatie	Ja	Ja			X	
5.5	Contact met overheidsinstanties	De organisatie moet contact met de relevante instanties leggen en onderhouden.	Ja	Ja			X	

5.6	Contact met speciale belangengroepen	De organisatie moet contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en beroepsverenigingen leggen en onderhouden.	Ja	Ja			X	
5.7	Informatie en analyses over dreigingen	Informatie- met betrekking tot informatiebeveiligingsdreigingen moet worden verzameld en geanalyseerd om informatie over dreigingen te produceren.	Ja	Ja			X	
5.8	Informatiebeveiliging en projectmanagement	Informatiebeveiliging moet worden geïntegreerd in projectmanagement.	Ja	Ja			X	
5.9	Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen	Er moet een inventarislijst van informatie en andere gerelateerde bedrijfsmiddelen, met inbegrip van de eigenaren, worden opgesteld en onderhouden.	Ja	Ja			X	
5.10	Aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmiddelen	Regels voor het aanvaardbaar gebruik van en procedures voor het omgaan met informatie en andere gerelateerde bedrijfsmiddelen moeten worden geïdentificeerd, gedocumenteerd en geïmplementeerd.	Ja	Ja			X	
5.11	Retourneren van bedrijfsmiddelen	Personeel en andere belanghebbenden, al naargelang de situatie, moeten alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst retourneren.	Ja	Ja			X	
5.12	Classificeren van informatie	Informatie moet worden geclassificeerd volgens de informatiebeveiligingsbehoeften van de organisatie, op basis van de eisen voor vertrouwelijkheid, integriteit, beschikbaarheid en relevante eisen van belanghebbenden.	Ja	Ja		X	X	

5.13	Labelen van informatie	Om informatie te labelen moet een passende reeks procedures worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	Ja	Ja			X	
5.14	Overdragen van informatie	Er moeten regels, procedures of overeenkomsten voor informatieoverdracht zijn ingesteld voor alle soorten van communicatiefaciliteiten binnen de organisatie en tussen de organisatie en andere partijen.	Ja	Ja		X	X	
5.15	Toegangsbeveiliging	Er moeten regels op basis van bedrijfs- en informatiebeveiligingseisen worden vastgesteld en geïmplementeerd om de fysieke en logische toegang tot informatie en andere gerelateerde bedrijfsmiddelen te beheersen.	Ja	Ja		X	X	
5.16	Identiteitsbeheer	De volledige levenscyclus van identiteiten moet worden beheerd.	Ja	Ja			X	
5.17	Authenticatie-informatie	De toewijzing en het beheer van authenticatie-informatie moet worden beheerst door middel van een beheerproces waarvan het adviseren van het personeel over de juiste manier van omgaan met authenticatie-informatie deel uitmaakt.	Ja	Ja			X	
5.18	Toegangsrechten	Toegangsrechten voor informatie en andere gerelateerde bedrijfsmiddelen moeten worden verstrekt, beoordeeld, aangepast en verwijderd overeenkomstig het onderwerpspecifieke beleid en de regels inzake toegangsbeveiliging van de organisatie.	Ja	Ja			X	

5.19	Informatiebeveiliging en leveranciersrelaties	Er moeten processen en procedures worden vastgesteld en geïmplementeerd om de informatiebeveiligingsrisico's in verband met het gebruik van producten of diensten van de leverancier te beheersen.	Ja	Ja			X	
5.20	Adresseren van informatiebeveiliging in leveranciersovereenkomsten	Relevante informatiebeveiligingseisen moeten worden vastgesteld en met elke leverancier op basis van het type leveranciersrelatie worden overeengekomen.	Ja	Ja	X	X	X	
5.21	Beheren van informatiebeveiliging in de ICT-toeleveringsketen	Er moeten processen en procedures worden bepaald en geïmplementeerd om de informatiebeveiligingsrisico's in verband met de toeleveringsketen van ICT-producten en -diensten te beheersen.	Ja	Ja			X	
5.22	Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten	De organisatie moet de informatiebeveiligingspraktijken en de dienstverlening van leveranciers regelmatig monitoren, beoordelen, evalueren en veranderingen daaraan beheren.	Ja	Ja			X	
5.23	Informatiebeveiliging voor het gebruik van clouddiensten	Processen voor het aanschaffen, gebruiken, beheren en beëindigen van clouddiensten moeten overeenkomstig de informatiebeveiligingseisen van de organisatie worden opgesteld.	Ja	Ja			X	
5.24	Plannen en voorbereiden van het beheer van informatiebeveiligings-incidenten	De organisatie moet plannen opstellen voor, en zich voorbereiden op, het beheren van informatiebeveiligingsincidenten door processen, rollen en verantwoordelijkheden voor het beheer van informatie[1]beveiligingsincidenten te definiëren, vast te stellen en te communiceren.	Ja	Ja			X	

5.25	Beoordelen van en besluiten over informatiebeveiligings-gebeurtenissen	De organisatie moet informatiebeveiligingsgebeurtenissen beoordelen en beslissen of ze moeten worden gecategoriseerd als informatiebeveiligingsincidenten.	Ja	Ja			X	
5.26	Reageren op informatiebeveiligings-incidenten	Op informatiebeveiligingsincidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures.	Ja	Ja			X	
5.27	Leren van informatiebeveiligings-incidenten	Kennis die is opgedaan met informatiebeveiligingsincidenten moet worden gebruikt om de beheersmaatregelen voor informatiebeveiliging te versterken en te verbeteren.	Ja	Ja			X	
5.28	Verzamelen van bewijsmateriaal	De organisatie moet procedures vaststellen en implementeren voor het identificeren, verzamelen, verkrijgen en bewaren van bewijs met betrekking tot informatiebeveiligingsgebeurtenissen.	Ja	Ja			X	
5.29	Informatiebeveiliging tijdens een verstoring	De organisatie moet plannen maken voor het op het passende niveau waarborgen van de informatiebeveiliging tijdens een verstoring.	Ja	Ja			X	
5.30	ICT-gereedheid voor bedrijfscontinuïteit	De ICT-gereedheid moet worden gepland, geïmplementeerd, onderhouden en getest op basis van bedrijfscontinuïteitsdoelstellingen en ICT-continuïteitseisen	Ja	Ja		X	X	
5.31	Wettelijke, statutaire, regelgevende en contractuele eisen	Wettelijke, statutaire, regelgevende en contractuele eisen die relevant zijn voor informatiebeveiliging en de aanpak van de organisatie om aan deze eisen te voldoen, moeten worden geïdentificeerd, gedocumenteerd en actueel gehouden.	Ja	Ja	X	X	X	
5.32	Intellectuele eigendomsrechten	De organisatie moet passende procedures implementeren om intellectuele eigendomsrechten te beschermen.	Ja	Ja	X		X	

5.33	Beschermen van registraties	Registraties moeten worden beschermd tegen verlies, vernietiging, vervalsing, toegang door onbevoegden en ongeoorloofde vrijgave.	Ja	Ja	X		X	
5.34	Privacy en bescherming van persoonsgegevens	De organisatie moet de eisen met betrekking tot het behoud van privacy en de bescherming van persoonsgegevens volgens de toepasselijke wet- en regelgeving en contractuele eisen identificeren en eraan voldoen.	Ja	Ja	X	X	X	
5.35	Onafhankelijke beoordeling van informatiebeveiliging	De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan, met inbegrip van mensen, processen en technologieën, moeten onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen, worden beoordeeld.	Ja	Ja		X	X	
5.36	Naleving van beleid, regels en normen voor informatiebeveiliging	De naleving van het informatiebeveiligingsbeleid, het onderwerpspecifieke beleid, regels en de normen van de organisatie moet regelmatig worden beoordeeld.	Ja	Ja	X	X	X	
5.37	Gedocumenteerde bedieningsprocedures	Bedieningsprocedures voor informatieverwerkende faciliteiten moeten worden gedocumenteerd en beschikbaar worden gesteld aan het personeel dat ze nodig heeft.	Ja	Ja			X	

6	Mensgerichte beheersmaatregelen							
6.1	Screening	De achtergrond van alle kandidaten voor een dienstverband moet worden gecontroleerd voordat ze bij de organisatie in dienst treden en daarna op gezette tijden worden herhaald. Hierbij moet rekening worden gehouden met de toepasselijke wet- en regelgeving en ethische overwegingen, en deze controle moet in verhouding staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's.	Ja	Ja			X	
6.2	Arbeidsovereenkomst	In arbeidsovereenkomsten moet worden vermeld wat de verantwoordelijkheden van het personeel en van de organisatie zijn wat betreft informatiebeveiliging.	Ja	Ja		X	X	
6.3	Bewustwording van, opleiding en training in informatiebeveiliging	Personeel van de organisatie en relevante belanghebbenden moeten een passende bewustwording van, opleiding en training in informatiebeveiliging en regelmatige updates over het informatiebeveiligingsbeleid, onderwerpspecifieke beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie, krijgen	Ja	Ja		X	X	
6.4	Disciplinaire procedure	Er moet een formele en gecommuniceerde disciplinaire procedure zijn om actie te ondernemen tegen personeel en andere belanghebbenden die zich schuldig hebben gemaakt aan een schending van het informatiebeveiligingsbeleid.	Ja	Ja		X	X	

6.5	Verantwoordelijkheden na beëindiging of wijziging van het dienstverband	Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband, moeten worden gedefinieerd, gehandhaafd en gecommuniceerd aan relevant personeel en andere belanghebbenden.	Ja	Ja		X	X	
6.6	Vertrouwelijkheids- of geheimhoudings-overeenkomsten	Vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie inzake de bescherming van informatie weerspiegelen, moeten worden geïdentificeerd, gedocumenteerd, regelmatig worden beoordeeld en ondertekend door personeel en andere relevante belanghebbenden.	Ja	Ja		X	X	
6.7	Werken op afstand	Wanneer personeel op afstand werkt, moeten er beveiligingsmaatregelen worden geïmplementeerd om informatie te beschermen die buiten het gebouw en/of terrein van de organisatie wordt ingezien, verwerkt of opgeslagen.	Ja	Ja			X	
6.8	Melden van informatiebeveiligings-gebeurtenissen	De organisatie moet voorzien in een mechanisme waarmee personeel waargenomen of vermoede informatiebeveiligings-gebeurtenissen tijdig via passende kanalen kan melden.	Ja	Ja		X	X	
7	**Fysieke beheersmaatregelen**							
7.1	Fysieke beveiligingszones	Zones die informatie en andere gerelateerde bedrijfsmiddelen bevatten, moeten worden beschermd door beveiligingszones te definiëren en te gebruiken	Ja	Ja			X	
7.2	Fysieke toegangsbeveiliging	Beveiligde zones moeten worden beschermd door passende toegangsbeveiligings-maatregelen en toegangspunten.	Ja	Ja		X	X	

7.3	Beveiligen van kantoren, ruimten en faciliteiten	Voor kantoren, ruimten en faciliteiten moet fysieke beveiliging worden ontworpen en geïmplementeerd.	Ja	Ja			X	
7.4	Monitoren van de fysieke beveiliging	Het gebouw en terrein moet voortdurend worden gemonitord op onbevoegde fysieke toegang.	Ja	Ja			X	
7.5	Beschermen tegen fysieke en omgevingsdreigingen	Er moet bescherming tegen fysieke en omgevingsdreigingen, zoals natuurrampen en andere opzettelijke of onopzettelijke fysieke dreigingen voor de infrastructuur, worden ontworpen en geïmplementeerd.	Ja	Ja			X	
7.6	Werken in beveiligde zones	Voor het werken in beveiligde zones moeten beveiligingsmaatregelen worden ontwikkeld en geïmplementeerd.	Ja	Ja			X	
7.7	'Clear desk' en 'clear sereen'	Er moeten ‘clear desk’-regels voor papieren documenten en verwijderbare opslagmedia en ‘clear screen’-regels voor informatieverwerkende faciliteiten worden gedefinieerd en op passende wijze worden afgedwongen.	Ja	Ja			X	
7.8	Plaatsen en beschermen van apparatuur	Apparatuur moet veilig worden geplaatst en beschermd.	Ja	Ja			X	
7.9	Beveiligen van bedrijfsmiddelen buiten het terrein	Bedrijfsmiddelen buiten het gebouw en/of terrein moeten worden beschermd.	Ja	Ja			X	
7.10	Opslagmedia	Opslagmedia moeten worden beheerd gedurende hun volledige levenscyclus van aanschaf, gebruik, transport en verwijdering overeenkomstig het classificatieschema en de hanteringseisen van de organisatie.	Ja	Ja			X	
7.11	Nutsvoorzieningen	Informatieverwerkende faciliteiten moeten worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door storingen in nutsvoorzieningen.	Ja	Ja			X	

7.12	Beveiligen van bekabeling	Voedingskabels en kabels voor het versturen van gegevens of die informatiediensten ondersteunen, moeten worden beschermd tegen onderschepping, interferentie of beschadiging.	Ja	Ja			X	
7.13	Onderhoud van apparatuur	Apparatuur moet op de juiste wijze worden onderhouden om de beschikbaarheid, integriteit en vertrouwelijkheid van informatie te garanderen.	Ja	Ja			X	
7.14	Vellig verwijderen of hergebruiken van apparatuur	Onderdelen van de apparatuur die opslagmedia bevatten, moeten worden gecontroleerd om te waarborgen dat gevoelige gegevens en gelicentieerde software zijn verwijderd of veilig zijn overschreven voordat ze worden verwijderd of hergebruikt.	Ja	Ja			X	
8	**Technologische beheersmaatregelen**							
8.1	User endpoint devices	Informatie die is opgeslagen op, wordt verwerkt door of toegankelijk is via 'user endpoint devices' moet worden beschermd.	Ja	Ja			X	
8.2	Speciale toegangsrechten	Het toewijzen en het gebruik van speciale toegangsrechten moet worden beperkt en beheerd.	Ja	Ja			X	
8.3	Beperking toegang tot informatie	De toegang tot informatie en andere gerelateerde bedrijfsmiddelen moet worden beperkt overeenkomstig het vastgestelde onderwerp specifieke beleid inzake toegangsbeveiliging.	Ja	Ja		X	X	
8.4	Toegangsbeveiliging op broncode	Lees- en schrijftoegang tot broncode, ontwikkelinstrumenten en softwarebibliotheken moet op passende wijze worden beheerd.	Ja	Ja			X	

8.5	Beveiligde authenticatie	Er moeten beveiligde authenticatie technologieën en -procedures worden geïmplementeerd op basis van beperkingen van de toegang tot informatie en het onderwerpspecifieke beleid inzake toegangsbeveiliging.	Ja	Ja			X	
8.6	Capaciteitsbeheer	Het gebruik van middelen moet worden gemonitord en aangepast overeenkomstig de huidige en verwachte capaciteitseisen.	Ja	Ja			X	
8.7	Bescherming tegen malware	Bescherming tegen malware moet worden geïmplementeerd en ondersteund door een passend gebuikersbewustzijn.	Ja	Ja			X	
8.8	Beheer van technische kwetsbaarheden	Er moet informatie worden verkregen over technische kwetsbaarheden van in gebruik zijnde informatiesystemen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden moet worden geëvalueerd en er moeten passende maatregelen worden getroffen.	Ja	Ja			X	
8.9	Configuratiebeheer	Configuraties, met inbegrip van beveiligingsconfiguraties, van hardware, software, diensten en netwerken moeten worden vastgesteld, gedocumenteerd, geïmplementeerd, gemonitord en beoordeeld.	Ja	Ja			X	
8.10	Wissen van informatie	In informatiesystemen, apparaten of andere opslagmedia opgeslagen informatie moet worden gewist als deze niet langer vereist is.	Ja	Ja			X	
8.11	Maskeren van gegevens	Gegevens moeten worden gemaskeerd overeenkomstig het onderwerpspecifieke beleid inzake toegangsbeveiliging en andere gerelateerde onderwerpspecifieke beleidsregels, en bedrijfseisen van de organisatie, rekening houdend met de toepasselijke wetgeving.	Ja	Ja			X	

8.12	Voorkomen van gegevenslekken (data leakage prevention)	Maatregelen om gegevenslekken te voorkomen moeten worden toegepast in systemen, netwerken en andere apparaten waarop of waarmee gevoelige informatie wordt verwerkt, opgeslagen of getransporteerd.	Ja	Ja			X	
8.13	Back-up van informatie	Back-ups van informatie, software en systemen moeten worden bewaard en regelmatig worden getest overeenkomstig het overeengekomen onderwerpspecifieke beleid inzake back-ups.	Ja	Ja		X	X	
8.14	Redundantie van informatieverwerkende faciliteiten	Informatieverwerkende faciliteiten moeten met voldoende redundantie worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	Ja	Ja		X	X	
8.15	Logging	Er moeten logbestanden waarin activiteiten, uitzonderingen, fouten en andere relevante gebeurtenissen worden geregistreerd, worden geproduceerd, opgeslagen, beschermd en geanalyseerd.	Ja	Ja		X	X	
8.16	Monitoren van activiteiten	Netwerken, systemen en toepassingen moeten worden gemonitord op afwijkend gedrag en er moeten passende maatregelen worden getroffen om potentiële informatiebeveiligingsincidenten te evalueren.	Ja	Ja		X	X	
8.17	Kloksynchronisatie	De klokken van informatieverwerkende systemen die door de organisatie worden gebruikt, moeten worden gesynchroniseerd met goedgekeurde tijdbronnen.	Ja	Ja			X	
8.18	Gebruik van speciale systeemhulpmiddelen	Het gebruik van systeemhulpmiddelen die in staat kunnen zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen, moet worden beperkt en nauwkeurig worden gecontroleerd.	Ja	Ja			X	

8.19	Installeren van software op operationele systemen	Er moeten procedures en maatregelen worden geïmplementeerd om het installeren van software op operationele systemen op veilige wijze te beheren.	Ja	Ja			X	
8.20	Beveiliging netwerkcomponenten	Netwerken en netwerkapparaten moeten worden beveiligd, beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	Ja	Ja		X	X	
8.21	Beveiliging van netwerkdiensten	Beveiligingsmechanismen, dienstverleningsniveaus en dienstverleningseisen voor alle netwerkdiensten moeten worden geïdentificeerd, geïmplementeerd en gemonitord.	Ja	Ja		X	X	
8.22	Netwerksegmentatie	Groepen informatiediensten, gebruikers en informatiesystemen moeten in de netwerken van de organisatie worden gesegmenteerd.	Ja	Ja			X	
8.23	Toepassen van webfilters	De toegang tot externe websites moet worden beheerd om de blootstelling aan kwaadaardige inhoud te beperken.	Ja	Ja			X	
8.24	Gebruik van cryptografie	Regels voor het doeltreffende gebruik van cryptografie, met inbegrip van het beheer van cryptografische sleutels, moeten worden gedefinieerd en geïmplementeerd.	Ja	Ja		X	X	
8.25	Beveiligen tijdens de ontwikkelcyclus	Voor het veilig ontwikkelen van software en systemen moeten regels worden vastgesteld en toegepast.	Ja	Ja			X	
8.26	Toepassingsbeveiligings-eisen	Er moeten eisen aan de informatiebeveiliging worden geïdentificeerd, gespecificeerd en goedgekeurd bij het ontwikkelen of aanschaffen van toepassingen.	Ja	Ja			X	

8.27	Veilige systeemarchitectuur en technische uitgangspunten	Uitgangspunten voor het ontwerpen van beveiligde systemen moeten worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle activiteiten betreffende het ontwikkelen van informatiesystemen.	Ja	Ja			X	
8.28	Vellig coderen	Er moeten principes voor veilig coderen worden toegepast op softwareontwikkeling.	Ja	Ja		X	X	
8.29	Testen van de beveiliging tijdens ontwikkeling en acceptatie	Processen voor het testen van de beveiliging moeten worden gedefinieerd en geïmplementeerd in de ontwikkelcyclus.	Ja	Ja			X	
8.30	Uitbestede systeemontwikkeling	De organisatie moet de activiteiten in verband met uitbestede systeemontwikkeling sturen, bewaken en beoordelen.	Nee	Nvt				Software ontwikkeling is niet uitbesteedt.
8.31	Scheiding van ontwikkel-, test en productieomgevingen	Ontwikkel-, test- en productieomgevingen moeten worden gescheiden en beveiligd.	Ja	Ja		X	X	
8.32	Wijzigingsbeheer	Wijzigingen in informatieverwerkende faciliteiten en informatiesystemen moeten onderworpen zijn aan procedures voor wijzigingsbeheer.	Ja	Ja			X	
8.33	Testgegevens	Testgegevens moeten op passende wijze worden geselecteerd, beschermd en beheerd.	Ja	Ja			X	
8.34	Bescherming van informatiesystemen tijdens audits	Audittests en andere auditactiviteiten waarbij operationele systemen worden beoordeeld, moeten worden gepland en overeengekomen tussen de tester en het verantwoordelijke management.	Ja	Ja			X	

The security measures are applied to the activities specified in Appendix 1. The application of location-bound security measures depends on the actual location where the work is performed.

The security measures referred to in this appendix apply exclusively to the physical locations of the processor, the hardware, the internal network connections and the organisation and persons for which/whom the processor is responsible and who are under his/her control.