ADDENDUM TO SUPPLIER AGREEMENT CONCERNING INFORMATION SECURITY

Between the undersigned

VZW Onze-Lieve-Vrouw of Troost, operator of A.Z. Sint-Blasius, with registered office at 9200 Dendermonde, Kroonveldlaan 50, VAT no. BE0411.975.133, lawfully represented in accordance with its articles of association by ..... [name], General Director,
Hereinafter referred to as the “Hospital”

AND

……

……

……..... [Supplier details to be completed]

Hereinafter referred to as the “Supplier”

Hereinafter jointly referred to as the “Parties”

Whereas

The Supplier provides services for the Hospital, as described in the Basic Agreement; these services may have an impact on the security of information and systems; and the Parties wish, through this Addendum, to establish the necessary organisational and technical measures to ensure an appropriate level of information security.

the following has been agreed:

1. DEFINITIONS

1.1 For the purposes of this Addendum, the following definitions shall apply:

- **NIS2 legislation: Act of 26 April 2024 establishing a framework for the cybersecurity of network and information systems of general interest for public security. This Act is commonly referred to as the Belgian NIS2 Act. It transposes the European NIS2 Directive (EU) 2022/2555 into Belgian law.**

- **Basic Agreement: the agreement between the Hospital and the Supplier dated**

  ……..……..……..[date]

  relating to

  ……..……

  ……..…… [insert title of agreement and, where applicable, reference number]

1.2 The Supplier shall provide services to the Hospital on the basis of and as defined in the Basic Agreement.

2. SCOPE AND RELATIONSHIP WITH THE BASIC AGREEMENT

2.1 This Addendum forms an integral part of the Basic Agreement concluded between the Hospital and the Supplier. The provisions of this Addendum apply in full to all information systems made available by the Supplier in the context of the performance of the services under the Basic Agreement.

2.2 The provisions of this Addendum (and its Annexes) shall prevail over and replace any conflicting provisions concerning information security in the Basic Agreement.

3. APPROPRIATE TECHNICAL AND ORGANISATIONAL MEASURES

Purpose and normative framework

3.1 The Supplier shall implement and maintain appropriate and proportionate organisational measures (in addition to technical and operational measures) to prevent or minimise risks to the security of network and information systems and the impact of incidents on continuity of care and the healthcare services provided, in accordance with Title 3, Chapter 1 (Articles 30-33) of the Belgian NIS2 Act.

3.2 These measures shall follow an all-hazards risk-based approach and cover at least the elements of the Belgian NIS2 Act (transposing NIS2 Article 21), including: (a) policies on risk analysis and information-system security; (b) incident handling; (c) business continuity (backup, disaster recovery and crisis management); (d) supply-chain security; (e) security in acquisition, development and maintenance (including vulnerability management and disclosure); (f) policies and procedures for measuring effectiveness; (g) cyber hygiene and training; (h) cryptography/encryption; (i) personnel security, access control and asset management; (j) multi-factor authentication and secure communications.

Duty of care in the supply chain (supply-chain security)

3.3 The Supplier shall ensure that subcontractors and critical suppliers involved in the services apply at least equivalent NIS2-compliant measures, including contractual flow-down, an obligation to notify the Supplier of incidents in a timely manner, and audit and evidence obligations towards the Hospital.

3.4 The Supplier shall maintain an up-to-date supplier register including risk classification, security requirements and the results of periodic assessments (at least annually), and shall make it available to the Hospital on request for NIS2 compliance purposes.

Policy framework, governance and training

3.5 The Supplier shall demonstrably maintain formal and current policy documents, including ISMS policy, risk-management policy, incident and crisis procedures, BCM/DR plans, vulnerability-management and patching policies, encryption policy, identity and access-management policy, and data-classification policy.

3.6 The Supplier shall provide role-based training and regular awareness activities for all relevant staff, in particular administrators and privileged users, in accordance with the training and cyber-hygiene requirements under Title 3, Chapter 1, Article 30 of the NIS2 legislation.

Identity and access management (IAM) and privileged access

3.7 Strong authentication (MFA) is mandatory for all administrator accounts, remote access and all access to production and care-critical systems. Least privilege and segregation of duties shall be the guiding principles.

3.8 Logging and monitoring of security-relevant events shall be implemented (SIEM or equivalent), with a minimum retention period of 12 months for PAM sessions and correlation with detection and response capabilities. This retention period is a contractual specification for accountability and forensic investigation.

Encryption and data protection

3.9 Encryption at rest and in transit is mandatory for care-critical data. Key management shall be documented and separated from operational management channels.

3.10 During incidents and crisis situations, the Supplier shall use secure communication channels for voice, video, text and emergency communications.

Vulnerability management and secure development

3.11 The Supplier shall maintain a formal vulnerability-management process covering identification, risk-based prioritisation, known actively exploited vulnerabilities, patching within defined timeframes and vulnerability disclosure.

3.12 Where software is developed, the Supplier shall deliver "secure by design" and "secure by default", including change and release management with segregated environments, code reviews and, where applicable, availability of an SBOM to the Hospital.

Business continuity, backup and crisis management

3.13 **The Supplier's BCP/DRP** shall be aligned with the Hospital's services. At least one test shall be performed annually, including a tabletop exercise with the Hospital, with recovery objectives (RTO/RPO) that safeguard continuity of care and comply with the BCM obligation under Title 3, Chapter 1, Article 30.

3.14 **Supplier backups** shall be encrypted, offline/immutable where relevant, and periodically tested for recoverability.

INCIDENT MANAGEMENT and notification support (contractual, in support of NIS2 notification obligations)

3.15 The Supplier shall maintain a 24/7 incident-response process with a contact point and communication channels for the Hospital.

3.16 Contractual internal notification deadlines to the Hospital:

- **Within 4 hours:** initial warning containing key information (what happened, when, scope, preliminary impact and initial measures taken).
- **Within 24 hours:** update including an indication of whether the incident is suspected to be caused by unlawful or malicious acts, potential cross-border impact and initial indicators of compromise (if available), enabling the Hospital, as an essential entity, to comply in time with the 24-hour early warning under Article 34 of the Belgian NIS2 Act and the 72-hour incident notification under Article 35, in line with the NIS2 reporting framework.
- **Within one month after the initial notification or termination of the incident:** final report including root cause, impact analysis, mitigation measures applied and planned, and lessons learned.
- The Supplier shall fully cooperate in coordination with CCB/CERT.be if the Hospital decides to make a voluntary or mandatory national notification, including sharing relevant technical artefacts. The CCB is designated as the national cybersecurity authority and national CSIRT by the Royal Decree of 9 June 2024.

4. EVIDENCE, COMPLIANCE AND AUDITS

To demonstrate compliance with Article 3, the Supplier shall provide one or more of the following:

- CCB CyberFundamentals (CyFun®) label at the relevant level;
- ISO/IEC 27001 certificate with a scope covering the services and processing activities supplied to the Hospital, including the Statement of Applicability;
- an equivalent conformity assessment under the Royal Decree of 9 June 2024 by a recognised conformity assessment body (CAB);
- a recent independent assurance report (e.g. ISAE 3000/3402 Type 2) sufficiently covering the measures referred to in Article 3;
- completed self-assessment questionnaire in Annex 1.

The Hospital shall have the right, itself or through an independent third party, to conduct audits and/or penetration tests in a reasonable manner, subject to reasonable notice and confidentiality, in order to verify compliance with this Article. The Supplier shall cooperate and remedy identified deficiencies

within reasonable timeframes. This is aligned with the regular conformity assessments under Title 4 of the NIS2 Act and its implementing Royal Decree.

5. DOCUMENTATION AND INFORMATION TO THE HOSPITAL/AUTHORITIES

5.1 Upon request, the Supplier shall provide current documentation (risk registers, asset inventory, high-level network diagrams, BCM/DR test reports, training registers and audit reports) required for the Hospital's NIS2 obligations, including supervision and inspection by the CCB.

5.2 If the Supplier itself falls within the scope of the Belgian NIS2 Act, it shall confirm its registration with the CCB and, upon request, provide relevant references (registration ID, designated sector/subsector).

6. CLOUD PROVIDER AND CLOUD SERVICES (IF APPLICABLE)

Where the Supplier uses cloud services or itself provides cloud services in support of the services to the Hospital, the Supplier shall ensure that the cloud architecture and supply chain comply with the risk-management, business-continuity and supply-chain-security obligations under the NIS2 Act.
The Supplier shall provide the Hospital with an up-to-date overview of cloud services used (IaaS/PaaS/SaaS), cloud provider(s), relevant components (identity management, logging, backup/DR), data geography/regions and a shared-responsibility matrix.
For cloud administration, the Supplier shall at least apply MFA, least privilege, logging of administrative activities and change control.
Cloud incidents at the cloud provider affecting services to the Hospital are subject to the notification and cooperation arrangements in Article 3.

6.1 Data Protection

6.1.1 Data at Rest

6.1.1.1 The Supplier shall ensure that all data stored by or on behalf of the Hospital are permanently stored in encrypted form.

6.1.1.2 Decryption of such data is permitted only within a secure, isolated execution environment (confidential computing environment).

6.1.1.3 Data shall be fully re-encrypted before leaving this execution environment.

6.1.1.4 Data shall at no time leave the environment in readable form.

6.1.2 Data in Transit

6.1.2.1 The Supplier shall ensure that all transfers of data between systems, components and services take place exclusively through strongly secured and encrypted communication channels.

6.1.2.2 Decryption during transport is permitted only within a confidential execution environment.

6.1.2.3 Transmission of unencrypted or readable data over cloud networks is expressly prohibited.

6.1.3 Secure data exchange with the cloud platform

6.1.3.1 Communication between the Hospital's cloud application and the Supplier's cloud platform shall be configured so that confidentiality, integrity and authenticity of information are safeguarded throughout the entire data lifecycle.

6.2 Encryption keys, secrets and authentication credentials

6.2.1 Protection of encryption keys and secrets

6.2.1.1 Encryption keys and other secrets shall be generated, stored and used exclusively within a secure environment.

6.2.1.2 Encryption keys and secrets shall never leave the enclave in readable or reusable form.

6.2.1.3 The Supplier shall have no technical, logical or operational capability to access or extract these encryption keys or secrets.

6.2.2 Independent key management

6.2.2.1 Encryption keys and secrets shall be managed on a system to which the Supplier has no access.

6.2.2.2 This system shall not be managed, monitored or supported by the Supplier.

6.2.3 Authentication credentials

6.2.3.1 Authentication credentials (such as passwords, tokens, certificates and keys) shall be considered and treated as secrets.

6.2.3.2 The Supplier shall have no access to systems that manage authentication credentials or perform authentication.

6.3 Access management and identity

6.3.1 Restrictions applicable to the Supplier

6.3.1.1 The Supplier shall have no logical access to servers, virtual machines or enclaves in which Hospital data are processed.

6.3.1.2 This restriction also applies to administrator accounts, emergency accounts and the Supplier's internal authentication credentials.

6.3.2 Authentication and authorisation

6.3.2.1 The cloud application shall mandatorily use multi-factor authentication (MFA).

6.3.2.2 Access management shall be integrated with Azure Active Directory or an equivalent identity platform under the Hospital's control.

6.3.2.3 The Supplier shall have no access to systems that define or enforce authorisations.

6.4 Deletion of data

6.4.1 The Supplier guarantees that data shall be completely and irreversibly deleted from all storage when instructed by the Hospital.

6.4.2 These deletion procedures shall be regularly verified and attested by an independent external party.

6.4.3 The results of these attestations shall be made available to the Hospital on request.

6.5 Exit strategy and termination of services

6.5.1 Purpose of the exit strategy

The purpose of the exit strategy is to ensure that, upon termination or modification of the services, the Hospital can continue to use or migrate its data and applications securely, completely and without unreasonable impediments to another service provider or to its own infrastructure, while preserving confidentiality, integrity and availability.

6.5.2 Exit scenarios

The exit strategy shall apply in each of the following cases:

- termination or non-renewal of the agreement, regardless of cause;
- a material breach of contract by the Supplier;

- changes to the services that create an unacceptable risk to security or legal compliance;
- bankruptcy, cessation or transfer of all or part of the Supplier's activities;
- legal or regulatory obligations requiring migration or termination.

6.5.3 Portability of data and configurations

6.5.3.1 The Supplier shall enable the Hospital to obtain all data, metadata, configurations and logical structures necessary for continuation of the services in a structured, commonly used and machine-readable form.

6.5.3.2 The Supplier shall ensure that the data are supplied in a format that technically enables migration to an alternative platform without loss of functionality or data integrity.

6.5.3.3 The Supplier shall ensure that transfer takes place through secure and encrypted mechanisms equivalent to the security measures applied during the term of the agreement.

6.5.4 Security during the exit phase

6.5.4.1 Throughout the exit phase, all contractually agreed security measures shall remain fully applicable.

6.5.4.2 During migration and transfer, data shall continue to be processed and transported exclusively in encrypted form.

6.5.4.3 Encryption keys, secrets and authentication credentials shall remain under the exclusive control of the Hospital at all times and shall not be transferred to the Supplier.

6.5.5 Support by the Supplier

6.5.5.1 The Supplier shall provide reasonable and timely support in implementing the exit strategy, including:

- providing documentation;
- technical support for export and migration;
- answering questions concerning data structures and dependencies.

6.5.5.2 Such support shall not be made subject to additional commercial conditions that unreasonably delay or obstruct the exit.

6.5.6 Deletion of data after exit

6.5.6.1 Following successful and complete transfer of the data, the Supplier shall confirm in writing that all Hospital data have been irreversibly deleted from its systems, including backups and redundant storage.

6.5.6.2 Such deletion shall take place within an agreed timeframe and in accordance with demonstrably secure procedures.

6.5.6.3 Upon request, the Supplier shall provide a statement or certificate demonstrating that deletion has effectively been carried out.

6.5.7 Continuity and availability

6.5.7.1 The Supplier shall ensure that availability of the services is not reduced without valid reason during the exit period.

6.5.7.2 The exit strategy shall not cause unexpected interruptions or loss of access to data, except where strictly necessary for the secure execution of the exit.

6.5.8 Periodic testing

6.5.8.1 The Hospital shall have the right to have the feasibility of the exit strategy periodically tested.

6.5.8.2 The Supplier shall cooperate with such tests, including carrying out a controlled exit or migration simulation where this can reasonably be expected.

6.5.9 Priority and enforceability

6.5.9.1 The provisions of this Article shall prevail over conflicting exit or termination provisions in other documents.

6.5.9.2 Failure to comply with this Article shall be considered a material breach of the agreement.

7. ARTIFICIAL INTELLIGENCE (IF APPLICABLE)

Where the Supplier uses AI or itself provides AI services in support of the services to the Hospital, the Supplier shall ensure that the AI components comply with the obligations under the AI Act. Where applicable, the questionnaire in Annex 2 shall be completed.

Agreed and executed in duplicate at ……..

on ……..….

[Name] [Name]

The Hospital **Supplier**

Annexes

Annex 1: Information Security – Self-Assessment Questionnaire
Annex 2: Questionnaire for procurement files containing an AI component

QUESTIONNAIRE ON THE PRESENCE AND EFFECTIVENESS OF ORGANISATIONAL AND TECHNICAL MEASURES FOR INFORMATION SECURITY

To be completed by the Supplier
Answer each question and state (by title) which supporting documents you have available.
The answers must also cover processing activities performed by subcontractors.

QUESTIONS	NO	YES	TESTED	SUPPORTING DOCUMENTS	Brief explanation
Description of the service					
Is the documentation concerning the service provided current and accurate?					
Organisational Measures					
ISO 5.1 – Is there a clear security policy covering all domains of ISO 27001/27002, taking into account the described dimensions to be considered, and is this known to employees?					
ISO 5.2 – Are roles and responsibilities defined, in particular for the CISO, DPO, operational management and incident management?					
ISO 5.3 – Is segregation of duties applied to prevent unauthorised actions?					
ISO 5.4 – Is the information-security policy formally approved and periodically reviewed by management?					
ISO 5.7 – Are structured threat analyses used to safeguard information security?					
ISO 5.8 – Is information security incorporated into project management?					
ISO 5.10 – Is there a policy on acceptable use of information and associated assets?					

ISO 5.12/5.13 – Is classification of data and systems applied?					
ISO 5.14 – Which formal rules and technical measures do you use to exchange information securely and traceably with internal and external parties?					
ISO 5.15/5.16/5.17/5.18 – Is strict user and access management in place, both for ordinary users and privileged administrators?					
ISO 5.19 – Are contractual obligations flowed down one-to-one to your subcontractors and do you monitor them at least annually?					
ISO 5.20 – Are all important activities, particularly administrator activities, recorded in immutable audit trails accessible to the Hospital?					
ISO 5.21/5.22/5.23 – Do you have clear rules concerning the delivery and use of software and hardware and security testing, applicable to every change?					
ISO 5.24 – Is there a policy and are there clear systems and processes for managing and coordinating security incidents?					
ISO 5.29 / ISO 5.30 – Do you have a plan for continuity of information security in the event of a disaster/disruption and is it tested?					
ISO 5.31 – Does the organisation maintain a current and documented overview of all relevant legal, regulatory and contractual security requirements, and is compliance periodically checked?					
ISO 5.32 – Does the organisation use documented procedures to protect intellectual-property rights and prevent the use of illegal software or unauthorised copies?					
ISO 5.34 – Are you familiar with and do you apply the rules on privacy and personal-data protection?					

ISO 5.35 – Is compliance of information security with the defined security requirements independently verified (e.g. internal or external audit)?					
ISO 5.36 – How is compliance with information-security policies, rules and standards ensured?					
Personnel Measures					
ISO 6.1 / 6.2 / 6.3 – Are there clear rules and supervision regarding the conduct of privileged administrators, and are security rules repeated annually in their training?					
ISO 6.3 – Are employees systematically trained and informed about risks and the secure handling of information?					
ISO 6.4/6.5/6.6 – Are there clear rules for non-compliant behaviour, changes of role or departure from the company? Are all employees bound by a confidentiality clause?					
ISO 6.7 / 6.8 – Are there clear rules for remote working (only through the processor's systems) and for reporting actual or potential security incidents?					
Physical Measures					
ISO 7.1/7.2/7.3/7.4 – Is access to systems, and the systems used for administration, adequately secured?					
ISO 7.5/7.6/7.7/7.8/7.10/7.11 – Are adequate measures in place that in principle make unauthorised access to systems and data carriers impossible?					
ISO 7.14 – Is cryptographic erasure or physical destruction used to guarantee that data are permanently deleted and/or hardware destroyed?					
Technological Measures					

ISO 8.1 – Is all information stored on, processed by or accessible through user endpoint devices (laptops, smartphones and tablets) adequately protected in accordance with the information-security policy?					
ISO 8.2 / ISO 8.3 / ISO 8.4 – Do you have a separate privileged access management (PAM) environment? Is a VPN used for remote administrative access? Is access restricted on a need-to-know basis?					
ISO 8.5 – Do you apply strong authentication to all processes and MFA to all privileged access?					
ISO 8.7 / 8.8 – Are your systems maximally protected against malware? Do you adequately test your systems for vulnerabilities?					
ISO 8.10 / 8.11 / 8.12 / 8.13 – Do you adequately protect data in accordance with their CIA classification levels?					
ISO 8.14 – Do you have the necessary backup and disaster-recovery systems in accordance with the CIA classification?					
ISO 8.15/8.16 – Do you have adequate logging and monitoring to detect security incidents?					
ISO 8.19 – Do you have a security policy for downloading and installing software?					
ISO 8.20 / 8.21 / 8.22 – Is there a policy for access to networks and network services, and is your infrastructure designed according to good practice to adequately segregate data and systems?					
ISO 8.24 – Do you apply adequate cryptographic measures where necessary, such as signing or encryption?					
ISO 8.25 / 8.26 / 8.27 / 8.28 / 8.29 – Do you have a software delivery pipeline that validates every code/configuration change for errors/non-conformities?					
ISO 8.33 – Do you have a policy to protect and anonymise test data?					

The Supplier,	
Name and position of the person signing on behalf of the Supplier (*legal representative*)	
Date	
I declare that the answers are correct and do not conceal any material deficiencies. I undertake to provide the supporting documents in the event of an audit.	Signature

ANNEX 2 – QUESTIONNAIRE FOR PROCUREMENT FILES CONTAINING AN AI COMPONENT

As the Hospital must comply with AI legislation and regulations (including the EU AI Act) and must always perform a thorough evaluation of all AI applications in the healthcare environment, you are requested to answer the questions below. This provides the Hospital with an initial high-level understanding of the AI functionality of the product and/or software.

Where relevant, distinguish in your answers between data used to train the model and data used in the application.

1. Type of AI functionality

- Can you indicate whether and to what extent the product uses AI/self-learning algorithms?
- What is the core functionality performed by the AI system (diagnostics, workflow optimisation, decision-making, monitoring, image recognition, etc.)?
- Is your AI system based on a general-purpose AI model capable of competently performing a wide range of different tasks? This does not apply if you use third-party AI models. Examples include:
  - Large language models (LLMs).
  - Text-to-image or text-to-video models.
  - Large vision models.
  - Multimodal models?
- Which Hospital data does the AI system use (cf. the overview in the attached Table 1)?
- To which category does the AI system belong under the AI Act?
  - Unacceptable
  - High risk
  - Limited risk
  - No risk

2. Operation and training of the AI system

- Can the AI system or Supplier explain how decisions or outputs were produced, including all relevant steps and the information on which the system relies (cf. transparency obligations under the EU AI Act)?
- On which data was the AI trained (e.g. patient data, demographic data, images)? Is the training specifically based on European or international datasets?
- Is the AI system continuously adjusted/self-learning or is it a statically trained model?
- If so, are Hospital data or data of Hospital patients used to further train or adjust the AI algorithm?
- What limitations does the AI system have? Please be specific.

3. Kill switch and safety

- Is there a kill switch / is the Hospital required to use the AI system if it does not wish to? Does the accompanying documentation explain how to switch to an alternative process?
- How are accuracy and validation ensured and bias in AI outputs prevented? Is documentation available?
- Is documentation available on clinical validation studies or CE marking, where relevant?
- Is there certification for the AI system, e.g. NIST?
- What measures are implemented to prevent the AI system from producing harmful, misleading or clinically unsafe output?
- How do you protect the AI system against AI security risks such as model poisoning or prompt-injection attacks?

4. Risks and risk classification

- Has the product already been classified in a risk class under the AI Act or medical-device legislation (MDR)?
- What class is it, how is this justified and is supporting documentation available?
- What risk-mitigation measures are taken, including insurance, exclusion of certain data or restriction of certain processing activities?
- Describe the exit procedure: what steps are foreseen to return our data (and, where relevant, AI models) in a usable format upon contract termination?
- Do you support export and portability of data or configurations in structured, machine-readable formats?

5. Data storage and protection

- How do you address privacy and data protection in relation to AI?
- Can you confirm that you will not apply AI to our data or patient data without our explicit consent?
- Can you confirm that no patient or Hospital data will be used to train the AI system?

6. Integration and use in the workflow

- How is the AI-based functionality integrated into daily practice (e.g. decision support in the EHR, standalone device, etc.)?
- Is training or guidance provided for those responsible for the application and for end users, and how is this organised?

7. Implementation, testing, maintenance and updates

- Who is responsible for this?
- Can the AI model be adapted to our specific needs? Who would do this and what would the costs/SLA look like?
- Is a human-oversight mechanism implemented?
  - Is the AI system designed so that human intervention remains possible before decisions with critical consequences?
  - Are safeguards in place to ensure that human oversight can be effectively exercised (e.g. clear explanations, timely warnings, override options)?
- What type of support do you provide to users to use the AI functionalities effectively?
- How are updates or new versions of the AI algorithm rolled out and communicated?
- Is there a process for reporting and following up potential problems or incidents?

The Hospital would like to receive your answers to these questions in order to make an initial assessment. On that basis, the Hospital can determine whether a more in-depth risk analysis, including a formal AI risk assessment, is required.

Table 1: Overview of possible data

Patient
Patient data in the EHR
Administrative identification data
Financial data
Social data and data on education and occupation
Psychiatric data
Health data
Data relating to relatives in a record
Third-party data in a record
Genetic data
Biometric data
Data concerning fertility and sexuality

Judicial/criminal data
National Register number
Racial or ethnic data, political opinions, beliefs
Data from non-medical sensors (image, sound, etc.)
GPS location data
Consents and care relationships
Insurability
Complaints
Employee
Employee data in the EHR
Administrative personnel data
Financial data
Social data and data on education and occupation
Employee health data
Judicial/criminal data
Evaluations and assessments
Complaints
Biometric data
National Register number
Visitor / Other
Administrative data
Financial data
GPS location data
Data from non-medical sensors (image, sound, etc.)
Data from online traffic
Other:

The Supplier,	
Name and position of the person signing on behalf of the Supplier (*legal representative*)	
Date	
I declare that the answers are correct and do not conceal any material deficiencies.	Signature