Assurance report

Intect ApS

ISAE 3402 type 1 assurance report on IT general controls related to the Payroll Platform as per 15 December 2025

Grant Thornton | www.grantthornton.dk
Lautrupsgade 11, 2100 København Ø
CVR: 34 20 99 36 | Tlf. +45 33 110 220 | mail@dk.gt.com

January 2026

Table of contents

Section 1: Intect ApS' statement 1

Section 2: Independent service auditor's assurance report on the description of controls and their design 3

Section 3: Description of Intect ApS' services in connection with the Payroll Platform 5

Section 4: Control objectives, controls, and service auditor testing 11

Section 1: Intect ApS' statement

The accompanying description has been prepared for customers who have used Intect ApS' Payroll Platform, and their auditors who have a sufficient understanding to consider the description along with other information about controls operated by customers themselves, when obtaining an understanding of customers' information systems relevant to financial reporting.

Intect ApS is using the following subservice organisations: Microsoft Azure, GitHub and YouTrack This assurance report is prepared in accordance with the carve-out method and Intect ApS' description does not include control objectives and controls within Microsoft Azure, GitHub and YouTrack. Certain control objectives stated in the description can only be achieved, if the subservice organisation's controls as assumed in the design of our controls, are appropriately designed and implemented. The description does not include control activities performed by subservice organisations.

Some of the control objectives stated in Intect ApS' description in Section 3 of IT general controls, can only be achieved if the complementary user entity controls with the customers have been appropriately designed and works effectively with the controls with Intect ApS. The report does not include the appropriateness of the design and operating effectiveness of these complementary user entity controls.

Intect ApS confirms that:

(a) The accompanying description in Section 3 fairly presents the IT general controls related to Intect ApS' Payroll Platform, processing customer transactions as per 15 December 2025.

The criteria used in making this statement were that the accompanying description:

(i) Presents how the system was designed and implemented, including:

- The type of services provided
- The procedures within both information technology and manual systems, used to manage IT general controls
- Relevant control objectives and controls designed to achieve these objectives
- Controls that we assumed, in the design of the system, would be implemented by user entities, and which, if necessary, to achieve the control objectives stated in the accompanying description, are identified in the description along with the specific control objectives that cannot be achieved by us alone
- Services provided by subservice organisations, including whether they are included according to the inclusive method or the carve-out method
- Other aspects of our control environment, risk assessment process, information system and communication, control activities, and monitoring controls that were relevant to IT general controls

(ii) Does not omit or distort information relevant to the scope of the system being described, while acknowledging that the description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the system that each individual customer may consider important in their own particular environment

(b) The controls related to the control objectives stated in the accompanying description were suitably designed as per 15 December 2025, if relevant controls with subservice organisations were implemented and the customers have performed the complementary user entity controls, assumed in the design of Intect ApS' controls as per 15 December 2025. The criteria used in making this statement were that:

(i) The risks that threatened achievement of the control objectives stated in the description were identified

(ii) The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved

Herlev, 5 January 2026
Intect ApS

Frants Moraitis
CEO

Section 2: Independent service auditor's assurance report on the description of controls and their design

To Intect ApS, their customers and their auditors.

Scope

We have been engaged to report on Intect ApS' description in Section 3 of Intect ApS' Payroll Platform as per 15 December 2025 (the description) and on the design and operation of controls related to the control objectives stated in the description.

Intect ApS is using the subservice organisations Microsoft Azure, GitHub and YouTrack. This assurance report is prepared in accordance with the carve-out method and Intect ApS' description does not include control objectives and controls within Microsoft Azure, GitHub and YouTrack. Certain control objectives in the description can only be achieved, if the subservice organisations' controls, assumed in the design of Intect ApS controls, are suitably designed and operationally effective. The description does not include control activities performed by the subservice organisation.

Some of the control objectives stated in Intect ApS' description in Section 3 of IT general controls, can only be achieved if the complementary user entity controls with the customers have been appropriately designed and works effectively with the controls with Intect ApS. The report does not include the appropriateness of the design and operating effectiveness of these complementary user entity controls.

Intect ApS' responsibility

Intect ApS is responsible for preparing the description (Section 3) and accompanying statement (Section 1) including the completeness, accuracy, and method of presentation of the description and statement. Additionally, Intect ApS is responsible for providing the services covered by the description; stating the control objectives; and for the design, implementation, and effectiveness of operating controls for achieving the stated control objectives.

Grant Thornton's independence and quality control

We have complied with the independence and other ethical requirements of the International Ethics Standards Board for Accountants' International Code of Ethics for Professional Accountants issued by the International Ethics Standards Board for Accountants (IESBA Code), which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour and ethical requirements applicable to Denmark. Grant Thornton applies International Standard on Quality Management 1, ISQM 1, requiring that we maintain a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

Auditor's responsibility

Our responsibility is to express an opinion on Intect ApS' description (Section 3) as well as on the design of the controls related to the control objectives stated in that description based on our procedures. We conducted our engagement in accordance with ISAE 3402, "Assurance Reports on Controls at a Service Organisation", issued by International Auditing and Assurance Standards Board (IASSB).

This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are suitably designed.

An assurance engagement to report on the description and design of controls at a service organisation involves performing procedures to obtain evidence about the disclosures in the service organisation's description of its system, and the design of controls.

The procedures selected depend on the service supplier's auditor's judgement, including the assessment of the risks that the description is not fairly presented, and that controls are not suitably designed.

Our actions have included test of the implementation of such controls, that we regard as necessary to obtain a reasonable assurance, that the control objectives stated in the description were obtained.

An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein, and the suitability of the criteria specified by the service organisation and described in Section 1.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Limitations of controls at a service organisation

Intect ApS' description in Section 3, is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the systems that each individual customer may consider important in their own particular environment. Also, because of their nature, controls at a service organisation may not prevent or detect all errors or omissions in processing or reporting transactions.

Opinion

Our opinion has been formed on the basis of the matters outlined in this report. The criteria we used in forming our opinion are those described in Intect ApS' Section 1 and based on this it is our opinion, in all material respects:

(a) the description fairly presents how Intect ApS' Payroll Platform was designed and implemented as per 15 December 2025.

(b) the controls related to the control objectives stated in the description were suitably designed and implemented as per 15 December 2025

Description of tests of controls

The specific controls tested, and the nature, timing and results of these tests are listed in the subsequent main section (Section 4) including control objectives, test, and test results.

Intended users and purpose

This assurance report is intended only for customers who have used Intect ApS' Payroll Platform and the auditors of these customers, who have a sufficient understanding to consider the description along with other information, including information about controls operated by customers themselves. This information serves to obtain an understanding of the customers' information systems, which are relevant for the financial reporting.

Herlev, 5 January 2026

Grant Thornton
Godkendt Revisionspartnerselskab

Kristian Randløv Lydolph
State Authorised Public Accountant

Andreas Moos
Partner, CISA, CISM

Section 3: Description of Intect ApS' services in connection with the Payroll Platform

Introduction

The following is a description of Intect's services, which are included in the IT general controls covered by this assurance report. The report includes general processes, system setups and control activities applied by Intect in relation to the operation of its payroll platform ("the Platform").

Processes, system setups and controls that are individually agreed with specific customers are not included in this report. Any assessment of customer-specific configurations or processes will be addressed in separate assurance reports, if applicable. Controls embedded directly within customer-managed application systems are not included in this report.

The object of this description is to provide information to Intect's customers and their auditors concerning the requirements laid down in the International Standard on Assurance Engagements (ISAE 3402) regarding controls at a service organisation.

The Platform is offered as a standardised SaaS solution and is used by customers across multiple industries. Intect is responsible for operating, maintaining and securing the platform, including hosting, infrastructure management, monitoring, backup, change management and information security controls.

Customer responsibilities include, among other things, administration of customer-specific data, user access management within the application, and approval of payroll-related transactions.

The infrastructure in scope of this description consists of Intect's cloud-based production environment hosted on Microsoft Azure within the EU.

The primary systems operated on the infrastructure in scope include:

- Intect Payroll Platform (SaaS application) including the surrounding technical environments and supporting services.

Intect has established an IT control environment designed to support the secure and reliable operation of the Platform. The control environment is based on ISO 27002:2022 and includes organisational, people, physical and technological controls.

Use of subservice organisations

Intect is using Microsoft in the delivery of the Intect Payroll service. Intect selects and manages this subservice organisation in accordance with applicable data protection requirements.

This ISAE 3402 report has been prepared using the carve-out method. Accordingly, the control objectives and related controls of subservice organisations and their sub-suppliers are excluded from the scope of this report.

Customers may obtain assurance over the services provided by these subservice organisations through independent assurance reports issued by the relevant providers.

Risk management

Intect performs risk management as an integrated part of its information security and IT operations. Risks related to information security, systems and business processes are identified and assessed on an ongoing basis.

Overall risk assessments are performed at least annually and when significant changes occur.

The risk assessments cover critical infrastructure, applications and supporting processes.

Based on the risk assessments, Intect determines appropriate control objectives and implements measures to maintain a stable and secure operation of its services.

The risk management approach is aligned with ISO 27002:2022 and supports continuous improvement of the control environment.

Organisation of information security

The organisation of it-security is based upon Intects IT-security policy and origins from ISO27002:2022, which contains the following main areas:

5	Organisational controls
6	People controls
7	Physical controls
8	Technological controls

Management of information security within the individual areas, are described below.

Control objectives and controls, chosen by Intect, are also stated in the summary in Section 4.

Intect has established clear roles and responsibilities for information security to ensure effective governance and control of security activities. Responsibility for information security is anchored in management and supported by documented policies and procedures.

Information security policies are established in alignment with ISO27002:2022 and are reviewed on a regular basis. The policies provide employees with clear guidelines regarding acceptable conduct and security responsibilities.

All employees are responsible for protecting Intect's information assets and complying with applicable security policies. Suspected or actual security incidents must be reported without delay and are documented, assessed and handled in accordance with established incident management procedures.

Control area 5: Organisational controls

Asset management

1 **Inventory of information and other associated assets** Intect maintains a central asset inventory, covering work equipment. The inventory is reviewed regularly.

2 **Acceptable use of information and other associated assets**: Intect has established IT and information security policies defining acceptable use of information and work equipment. This policy applies to all employees and must be acknowledged during onboarding and subsequently on an annual basis.

3 **Return of assets**: Intect has implemented procedures to ensure that company-issued assets are returned upon termination of employment. Logical access to systems and data is removed or adjusted immediately upon notice of termination or role change.

Access controls

4 **Access control**: Access to Intect's production environment is restricted based on the principle of least privilege and requires approval.
Access rights are regularly reviewed to ensure that access remains appropriate.

5 **Identity management**:
All employees are assigned a unique user account linked to an individual email address. Intect uses Microsoft Entra ID (Office 365 cloud-based identity management) as the primary directory service for user authentication.
Multi-factor authentication is enforced for access to Microsoft 365 services. User lifecycle management processes are in place to ensure timely provisioning, modification, and deprovisioning of user accounts.
Access to business systems is managed individually per system, as a centralised single sign-on solution is not implemented across all applications. Each system therefore maintains its own authentication and access controls.

6 **Access rights**: The granting of privileges is controlled in accordance with the regular user administration process. Privileges are only granted on a need-to-basis.

Supplier relationships

7 **Information security in supplier relationships**: Intect has established procedures to manage information security in supplier relationships. Suppliers undergo onboarding, including risk assessment. Critical suppliers are reassessed at least annually.

8 **Addressing information security within supplier agreements:** Information security requirements are addressed within supplier agreements, including security requirements and defined service level expectations.

9 **Monitoring, review and change management of supplier services:**
Intect monitors and reviews services delivered by suppliers and subservice organisations on an ongoing basis to ensure that they continue to meet contractual, operational, and information security requirements. This includes periodic reviews of service performance, incident handling, and relevant assurance documentation (e.g. ISAE/SOC reports), where available.

10 **Information security for use of cloud services**:
Intect uses cloud-based services as part of delivering the Intect Payroll. Information security requirements for cloud services are defined through contractual agreements and are aligned with applicable information security standards.
Intect ensures that appropriate technical and organisational measures are in place to protect the confidentiality, integrity, and availability of information processed in cloud environments, including access controls and incident management processes. Compliance is supported through ongoing oversight and review of relevant assurance reports provided by cloud service providers.

Incident management

11 **Information security incident management planning and preparation:** Intect maintains a documented incident response policy that defines roles, responsibilities and procedures for detecting, escalating, investigating and remediating information security incidents.
The plan is reviewed and tested at least annually.

12 **Assessment and decision on information security events**: Information security events are assessed based on severity, business impact and regulatory considerations.
Events classified as Critical incidents are escalated to management.

13 **Response to information security incidents**: Information security incidents are handled in accordance with documented procedures. Response activities, decisions and corrective actions are documented and retained.

14 **Learning from information security incidents:** Intect performs post-incident reviews for Critical information security incidents. Lessons learned are used to improve controls, procedures and preventive measures.

15 **Information security during disruption**: Intect maintains business continuity and disaster recovery plans to ensure continuation of payroll operations.

16 **Protection of records**: Operational logs, audit trails and financial records are retained according to contractual and regulatory requirements.

Control area 6: People controls

1 **Information security awareness, education, and training**
Intect ensures that all employees receive information security awareness training during onboarding and on an annual basis thereafter.

Control area 7: Physical controls

1 **Physical security perimeters:** Intect primarily operates from office environments with controlled physical access. All hosting environments are located within Microsoft Azure datacentres, which are protected by Microsoft's security controls.

2 **Physical entry**: Access to Intect's office facilities requires access cards, and visitor access is subject to escorting procedures.

3 **Securing offices, rooms, and facilities**: Offices, rooms and facilities are secured to prevent unauthorised access. Company devices are encrypted and protected by centrally managed security controls.

Control area 8: Technological controls

1 **Privileged access rights:** Privileged access rights are restricted to authorised personnel and protected by multi-factor authentication. Activities performed using privileged accounts are logged and periodically reviewed.

2 **Information access restrictions**: Access to information and systems is restricted based on job function and business need.

3 **Access to source code**: Access to source code repositories is limited to authorised development personnel and protected by multi-factor authentication. All changes are tracked using version control systems.

4 **Secure authentication**: Secure authentication mechanisms are enforced across systems, including strong password requirements and multi-factor authentication for employee and administrative access.

5 **Protection against malware**: Servers and endpoints are protected by centrally managed anti-malware and endpoint detection solutions, which are kept up to date.

6 **Management of technical vulnerabilities**: Intect identifies technical vulnerabilities through monitoring, advisories and vulnerability scanning. Vulnerabilities are assessed and remediated according to defined timelines.

7 **Information deletion**: Information is deleted or anonymised securely in accordance with data retention policies, contractual requirements and applicable legislation.

8 **Information backup**: Backups of production data are performed on a regular basis and stored in encrypted form. Backup restoration tests are conducted periodically.

9 **Logging**: System, access and security logs are collected centrally, protected against unauthorised modification and monitored for anomalies and security events.

10 **Use of privileged utility programs**: Use of privileged utility programs is restricted to authorised personnel and monitored to prevent misuse.

11 **Installation of software on operating systems**: Installation of software on operating systems is governed by internal policies and guidelines as set out in Intect's employee handbook. Employees are required to comply with these policies, and installation of software is subject to defined procedures and, where applicable, authorisation to ensure that only approved software is installed on operating systems.

12 **Networks security**: Network security is maintained through firewalls, segmentation and secure configuration of network components. External communication is encrypted.

13 **Security of network services:** Intect operates logically segregated network environments to support different purposes.

14 **Segregation of networks**: Production, test and development environments are logically segregated to reduce the risk of unauthorised access or changes.

15 **Use of cryptography**: Cryptographic controls are used to protect data in transit and at rest using industry-standard encryption protocols.

16 **Secure development life cycle**: Intect applies a secure development life cycle that integrates security requirements, reviews and testing throughout development activities.

17 **Secure system architecture and engineering principles**: System architecture follows security-by-design principles and least privilege.

18 **Secure coding**: Developers follow secure coding practices and use automated tools to identify and remediate vulnerabilities.

19 **Security testing in development and acceptance:** Security testing, including code analysis and vulnerability scanning, is performed prior to deployment to production.

20 **Separation of development, test, and production environments:** Development, test and production environments are separated, and only authorised personnel may deploy changes to production.

21 **Change management**: Changes follow a documented change management process that includes approval, testing and rollback procedures.

22 **Test information**: Test data does not include production personal data unless the data has been anonymised and explicitly approved.

Complementary user entity controls with the customers

The controls implemented by Intect are designed under the assumption that certain controls are established and operated by the customers.

The achievement of the control objectives described in this assurance report is therefore dependent on the customers implementing and maintaining appropriate complementary user entity controls.

- Customers are responsible for establishing and maintaining secure access to Intect Payroll, including the creation, administration and periodic review of user accounts. Customers must ensure that access credentials are kept confidential, are not shared with third parties.
- Customers are further responsible for ensuring that their own IT environment, including hardware, software, network connectivity, antivirus protection, firewalls and other relevant security measures, is adequate and up to date.
- Customers are responsible for cooperating with Intect by providing timely assistance, accurate and complete information, and access to relevant resources as required for the proper delivery of Intect Payroll.
- Customers must ensure that Intect Payroll is used in accordance with applicable terms, instructions and guidelines, that users are informed of the applicable conditions, and that errors or irregularities are reported to Intect without undue delay.
- Customers are solely responsible for the correctness, completeness and timeliness of all data entered into and processed by Intect Payroll, including payroll data, payment instructions, tax calculations and other financial information. Customers are required to perform appropriate reviews and controls of both input and output data, including post-processing reviews of payroll runs, and to maintain adequate procedures for backup and contingency handling, including manual procedures where relevant.
- Once access to Intect Payroll has been provided, the responsibility for the handling, protection and use of data rests with the customer. This includes responsibility for lawful use of the Product, compliance with applicable laws and regulations, and management of any third-party dependencies on the customer's side. Customers are also responsible for appointing authorized representatives who act as primary points of contact towards Intect.

The complementary user entity controls described above do not constitute an exhaustive list of all controls that may be required at the customer but represent controls that are considered necessary for Intects controls to operate effectively and for the control objectives in this assurance report to be achieved.

Section 4: Control objectives, controls, and service auditor testing

Purpose and scope

A description and the results of our tests based on the tested controls appear from the tables on the following pages. To the extent that we have identified significant weaknesses in the control environment or deviations therefrom, we have specified this.

This statement is issued according to the carve-out method and therefore does not include controls of Intect ApS' subservice organisations.

Controls, which are specific to the individual customer solutions, or are performed by Intect ApS' customers, are not included in this report.

Tests

We performed our test of controls at Intect ApS, by taking the following actions:

Method	General description
Inquiries	Interview with appropriate personnel at Intect ApS regarding controls. Inquiries have included questions on how controls are being performed.
Observation	Observing how controls are performed.
Inspection	Review and evaluation of policies, procedures and documentation concerning the performance of controls. This includes reading and assessment of reports and documents in order to evaluate whether the specific controls are designed in such a way, that they can be expected to be effective when implemented. Further, it is assessed whether controls are monitored and controlled adequately and with suitable intervals. The effectiveness of the controls is assessed by sample testing.
Re-performance	Re-performance of controls in order to verify that the control is working as assumed.

Test results

Below, we have listed the tests performed by Grant Thornton as basis for the evaluation of the IT general controls with Intect ApS.

A.5 Organisational controls			
Control objective: To ensure continuing suitability, adequacy, effectiveness of management direction and support for information security in accordance with business, legal, statutory, regulatory, and contractual requirements.			
No.	**Intect ApS' control**	**Grant Thornton's test**	**Test results**
5.9	*Inventory of information and other associated assets* An inventory of information and other associated assets, including owners, should be developed and maintained.	We have inspected that an inventory of assets, including owners, is developed and maintained.	No deviations noted.
5.10	*Acceptable use of information and other associated assets* Rules for the acceptable use and procedures for handling information and other associated assets should be identified, documented, and implemented.	We have inspected that a policy for accepted use of information and assets has been designed. We have inspected that the rules for acceptable use of information and assets have been implemented.	No deviations noted.
5.11	*Return of assets* Personnel and other interested parties as appropriate should return all the organisation's assets in their possession upon change or termination of their employment, contract, or agreement.	We have inspected that a process for return of assets has been designed. We have inspected that latest terminated personnel have returned assets to the organisation.	No deviations noted.

5. Organisational controls

Control objective: To ensure an appropriate protection of information considering the value of the information to the organisation.

No.	*Intect ApS' control*	*Grant Thornton's test*	*Test results*
5.15	*Access control* Rules to control physical and logical access to information and other associated assets should be established and implemented based on business and information security requirements.	We have inspected that an access management policy has been designed and updated. We have inspected that the access management policy has been implemented.	No deviations noted.
5.16	*Identity management* The full life cycle of identities should be managed.	We have inspected that identities are assigned unique user IDs that enable the traceability of actions performed. We have inspected that assignment of user access rights is granted based on the job function and an approval from the immediate superior. We have inspected that removal of user access rights is performed in a timely manner upon termination.	No deviations noted.
5.18	*Access rights* Access rights to information and other associated assets should be provisioned, reviewed, modified and removed in accordance with the organisation's topic-specific policy on and rules for access control.	We have inspected that assignment of user access rights is granted based on the job function and an approval from the immediate superior. We have inspected that removal of user access rights is performed in a timely manner upon termination. We have inspected that access rights have been reviewed on a regular basis and at least annually.	No deviations noted.
5.19	*Information security in supplier relationships* Processes and procedures should be defined and implemented to manage the information security risks associated with the use of supplier's products or services.	We have inspected that the procedure for managing supplier relationships and service agreements, contains requirements to mitigate risks connected with suppliers' access to assets.	No deviations noted.

No.	Intect ApS' control	Grant Thornton's test	Test results
5.20	*Addressing information security within supplier agreements* Relevant information security requirements should be established and agreed with each supplier based on the type of supplier relationship.	We have inspected that supplier agreements contain relevant information security requirements.	No deviations noted.
5.22	*Monitoring, review and change management of supplier services* The organisation should regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.	We have inspected that monitoring activities, covering outsourced supplier services, has been performed for all significant suppliers. We have inspected that any significant risks identified as part of the monitoring activities are followed up on.	No deviations noted.
5.23	*Information security for use of cloud services* Processes for acquisition, use, management and exit from cloud services should be established in accordance with the organisation's information security requirements.	We have inspected that policies for information security measures covering the use of cloud services have been defined and implemented.	No deviations noted.
5.24	*Information security incident management planning and preparation* The organisation should plan and prepare for managing information security incidents by defining, establishing, and communicating information security incident management processes, roles, and responsibilities.	We have inspected that an incident management procedure has been designed. We have inspected that roles and responsibilities related to the incident management procedure has been defined and made available to relevant employees.	No deviations noted.
5.25	*Assessment and decision on information security events* The organisation should assess information security events and decide if they are to be categorised as information security incidents.	We have inspected that a procedure for assessment and decision on information security events has been designed. We have inspected that information security events have been handled and categorised according to the procedure.	No deviations noted.

No.	Intect ApS' control	Grant Thornton's test	Test results
5.26	*Response to information security incidents* Information security incidents should be responded to in accordance with the documented procedures.	We have inspected the procedure for responding to information security incidents. We have inspected that the latest information security incident has been responded to according to the procedure.	No deviations noted.
5.27	*Learning from information security incidents* Knowledge gained from information security incidents should be used to strengthen and improve the information security controls.	We have inspected that a procedure for learning from information security incidents has been designed. We have inspected that security incidents have been registered in order to gain information to reduce probability of recurrence.	No deviations noted.
5.29	*Information security during disruption* The organisation should plan how to maintain information security at an appropriate level during disruption.	We have inspected that business contingency plans are designed and approved by management. We have inspected that the business contingency plans are made available to relevant employees.	No deviations noted.
5.33	*Protection of records* Records should be protected from loss, destruction, falsification, unauthorised access and unauthorised release.	We have inspected that logs collected are protected against manipulation or deletion.	No deviations noted.

6. People controls

Control objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

No.	Intect ApS' control	Grant Thornton's test	Test results
6.3	*Information security awareness, education and training* Personnel of the organisation and relevant interested parties should receive appropriate information security awareness, education and training and regular updates of the organisation's information security policy, topic-specific policies and procedures, as relevant for their job function.	We have inspected that an information security awareness programme has been established. We have inspected that the organisation's employees have completed the information security awareness training.	No deviations noted.

7. Physical controls

Control objective: To prevent unauthorised physical access, damage and interference to the organisation's information and other associated assets.

No.	Intect ApS' control	Grant Thornton's test	Test results
7.1	*Physical security perimeters* Security perimeters should be defined and used to protect areas that contain information and other associated assets.	We have inspected the procedure for physical protection of facilities and security perimeters. We have inspected relevant locations and their security perimeters to establish whether security measures have been implemented to prevent unauthorised access.	No deviations noted.
7.2	*Physical entry* Secure areas should be protected by appropriate entry controls and access points.	We have inspected the procedure for granting physical access. We have inspected access points and entry ways to establish, whether personal access cards are used to gain access to the office. We have inspected that alarms have been installed for physical access control and that these are active.	No deviations noted.

No.	Intect ApS' control	Grant Thornton's test	Test results
7.3	*Securing offices, rooms and facilities* Physical security for offices, rooms and facilities should be designed and implemented.	We have inspected that physical security has been applied to protect offices, rooms and facilities. We have inspected the processing facilities are not visible or audible from the outside.	No deviations noted.

8. Technological controls

Control objectives: To ensure that the allocation and use of privileged access rights have been restricted and controlled to reduce the risk of unauthorised access, changes to systems and inaccurate authentication.

No.	Intect ApS' control	Grant Thornton's test	Test results
8.2	*Privileged access rights* The allocation and use of privileged access rights should be restricted and managed.	We have inspected that a procedure for administration of privileged access rights has been designed. We have inspected that assignment of privileged access rights is granted based on an approval from the immediate superior. We have inspected that privileged access rights are restricted to a work-related need.	No deviations noted.
8.3	*Information access restriction* Access to information and other associated assets should be restricted in accordance with the established topic-specific policy on access control.	We have inspected that an access management policy and procedure have been designed and updated. We have inspected that assignment of user access rights is based on user groups and roles that comprise specific access restrictions, such as read, write, delete and execute. We have inspected that access to sensitive information is restricted to a work-related need. We have inspected that access rights have been reviewed on a regular basis and at least annually.	No deviations noted.

No.	Intect ApS' control	Grant Thornton's test	Test results
8.4	*Access to source code* Read and write access to source code, development tools and software libraries should be appropriately managed.	We have inspected that access to source code has been limited to employees with a work-related need.	No deviations notes.
8.5	*Secure authentication* Secure authentication technologies and procedures should be implemented based on information access restrictions and the topic-specific policy on access control.	We have inspected that a password management procedure has been designed. We have inspected that the password configuration settings are set in accordance with the defined procedure. We have inspected that multi-factor authentication is installed and enabled.	No deviations noted.

8. Technological controls

Control objective: To ensure correct and secure operation of information processing facilities.

No.	Intect ApS' control	Grant Thornton's test	Test results
8.7	*Protection against malware* Protection against malware should be implemented and supported by appropriate user awareness.	We have inspected that a procedure for protection against malware has been designed. We have inspected that anti-malware has been implemented on servers. We have inspected that anti-malware has been implemented on laptops.	No deviations noted.
8.8	*Management of technical vulnerabilities* Information about technical vulnerabilities of information systems in use should be obtained, the organisation's exposure to such vulnerabilities should be evaluated and appropriate measures should be taken.	We have inspected that a procedure for management of technical vulnerabilities has been designed. We have inspected that vulnerability scans are performed on a regular basis.	No deviations noted.

8. Technological controls

Control objective: To prevent unnecessary exposure of sensitive information and to comply with legal, statutory, regulatory and contractual requirements.

No.	Intect ApS' control	Grant Thornton's test	Test results
8.10	*Information deletion* Information stored in information systems, devices or in any other storage media should be deleted when no longer required.	We have inspected that a procedure for deletion of information has been designed. We have inspected that systems are configured to delete information automatically in accordance with the procedure. We have inspected that information is deleted upon disposal of media.	No deviations noted.

8. Technological controls

Control objective: To ensure the continuous operation of information processing facilities including the recovery from loss of data or systems.

No.	Intect ApS' control	Grant Thornton's test	Test results
8.13	*Information backup* Backup copies of information, software and systems should be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	We have inspected that a policy for backup of data has been designed. We have inspected that backup copies of are made continuously in accordance with the policy. We have inspected that daily backup reports are received from the backup system specifying whether the backup has been successfully completed. We have inspected that regular tests are performed of backup data to verify that the data can be restored from backup files.	No deviations noted.

8. Technological controls

Control objective: To record events, generate evidence, ensure the integrity of log information, prevent against unauthorised access, detect anomalous behaviour and identify information security events and incidents.

No.	Intect ApS' control	Grant Thornton's test	Test results
8.15	*Logging* Logs that record activities, exceptions, faults and other relevant events should be produced, stored, protected and analysed.	We have inspected that a procedure for log management has been designed. We have inspected that logs are configured in accordance with the procedure including, as a minimum, the caption of: - user IDs - system activities - dates, times and details of events We have inspected that logs collected are protected against manipulation or deletion.	No deviations noted.

8. Technological controls

Control objectives: To ensure the integrity of operational systems and application controls as well as prevent exploitation of technical vulnerabilities.

No.	Intect ApS' control	Grant Thornton's test	Test results
8.18	*Use of privileged utility programs* The use of utility programs that can be capable of overriding system and application controls should be restricted and tightly controlled.	We have inspected that access to maintain utility programs has been limited to users with a work-related need. We have inspected that any changes made to utility programs are logged.	No deviations noted.
8.19	*Installation of software on operational systems* Procedures and measures should be implemented to securely manage software installation on operational systems.	We have inspected that a procedure for installation of software on operational systems has been designed. We have inspected that server operating systems are patched in accordance with the procedure.	No deviations noted.

8. Technological controls

Control objectives: To ensure the protection of information in networks and its supporting information processing facilities.

No.	*Intect ApS' control*	*Grant Thornton's test*	*Test results*
8.20	*Network security* Networks and network devices should be secured, managed and controlled to protect information in systems and applications.	We have inspected that a network security policy has been designed. We have inspected that virtual private network (VPN) is used for secure encrypted connection with networks outside of the organisation. We have inspected that the network is monitored for anomalies and that these are followed up on.	No deviations noted.
8.21	*Security of network services* Security mechanisms, service levels and service requirements of network services should be identified, implemented and monitored.	We have inspected that a network security policy has been designed. We have inspected that firewalls and intrusion detection systems are installed on the network. We have inspected that the network is monitored for anomalies and that these are followed up on.	No deviations noted.
8.22	*Segregation of networks* Groups of information services, users and information systems should be segregated in the organisation's networks.	We have inspected that a network security policy has been designed. We have inspected that network segmentation is implemented dividing the network into multiple zones.	No deviations noted.
8.24	*Use of cryptography* Rules for the effective use of cryptography, including cryptographic key management, should be defined and implemented.	We have inspected that a policy defining rules for the use of cryptography has been defined. We have inspected that information is protected in accordance with the policy for cryptography.	No deviations noted.

8. Technological controls

Control objective: To ensure information security is designed and implemented within the secure development life cycle of software and systems.

No.	Intect ApS' control	Grant Thornton's test	Test results
8.25	*Secure development life cycle* Rules for the secure development of software and systems should be established and applied.	We have inspected that a procedure for secure development life cycle has been designed and applied.	No deviations noted.
8.27	*Secure system architecture and engineering principles* Principles for engineering secure systems should be established, documented, maintained and applied to any information system development activities.	We have inspected that the organisation has defined principles for information system development activities.	No deviations noted.
8.28	*Secure coding* Secure coding principles should be applied to software development.	We have inspected that a software development procedure has been designed. We have inspected that new software has been developed in accordance with the procedure.	No deviations noted.

8. Technological controls

Control objective: To validate if information security requirements are met when applications or code are deployed to the production environment.

No.	Intect ApS' control	Grant Thornton's test	Test results
8.29	*Security testing in development and acceptance* Security testing processes should be defined and implemented in the development life cycle.	We have inspected that development cases have been subject to system security testing.	No deviations noted.

8. Technological controls

Control objective: To ensure that changes to applications, database systems, and associated infrastructure are properly authorised, documented, tested, approved, and implemented in the production environment.

No.	Intect ApS' control	Grant Thornton's test	Test results
8.31	*Separation of development, test and production environments* Development, testing and production environments should be separated and secured.	We have inspected that development, testing and production environments are separated. We have inspected that segregation of duties has been established between employees with access to development, testing and production environments.	No deviations noted.
8.32	*Change management* Changes to information processing facilities and information systems should be subject to change management procedures.	We have inspected that a change management procedure has been designed. We have inspected that key stakeholders have approved changes prior to release into production. We have inspected that changes are tested based on established criteria prior to release into production.	No deviations noted.
8.33	*Test information* Test information should be appropriately selected, protected and managed.	We have inspected that sensitive information is protected by removal or masking procedures.	No deviations noted.

The signatures in this document are legally binding. The document is signed using Penneo™ secure digital signature. The identity of the signers has been recorded, and are listed below.

"By my signature I confirm all dates and content in this document."

Frants Ektora Moraitis
Underskriver 1
Serial number: 7a17a175-7e03-4676-9114-feb85a58b798
IP: 77.241.xxx.xxx
2026-01-06 10:39:49 UTC

Andreas Moos
Grant Thornton, Godkendt Revisionspartnerselskab CVR: 34209936
Underskriver 2
Serial number: 8ba4bf1c-2aac-4cbe-9a4b-48056ec67035
IP: 62.243.xxx.xxx
2026-01-06 11:37:40 UTC

Kristian Randløv Lydolph
Grant Thornton, Godkendt Revisionspartnerselskab CVR: 34209936
Underskriver 3
Serial number: 84758c07-82ce-4650-a48d-5224b246b5c4
IP: 62.243.xxx.xxx
2026-01-06 11:59:22 UTC