

Presentation of ScanNet's security environment

Version:

1.3

Date:


17. March 2021



ISO 27001

Deloitte.
ISAE 3402 Type 2

Table of Contents



Introduction:	page 3
Organisation of security:	page 3
Policies, procedures and standards:	page 3
Employee security:	page 3
Dedicated security and personal data competences:	page 3
Operational security - protection of customer data:	page 4
Emergency and disaster recovery:	page 4
Management of subcontractors:	page 5
Audit, compliance and independent third-party assessments:	page 5

The industry's leading programme for information security

Introduction

As a hosting provider, our most important security task is to take good care of your data and make sure that you always meet the security requirements of your customers.

Therefore, security is an area that we take very seriously - at all levels.

The purpose of this document is to give you an insight into how we secure our platform so, as a customer, you do not have to worry about security, but instead can spend time and energy on growing your business.

Organization of security

We have established an industry-leading information security programme (ISMS) that gives our customers the best protection and highest degree of confidence.

The program follows the ISO 27001 security standard, which we have been certified for since 2015.

Policies, procedures and standards

We have defined a set of policies, procedures and standards for how we operate in the company and take the best care of your data. The documents are regularly updated in line with the changing of the threat assessment. In this way we ensure that we always prioritize our efforts where they are needed the most.

How we prioritize the efforts depends on our risk assessment, which is updated regularly and forms the core of our information security programme.

Employee security

All employees and consultants with access to systems and facilities are subject to our security policies. Everyone undergoes compulsory training where they are presented with all relevant and current privacy and security topics. This occurs both upon commencement and continuously throughout their employment. The purpose is to equip employees so they can cope with actual threats against company and customer data.

In order to boost the overall level in the industry and to maintain own competences, our employees participate actively in communities and exchange of experience groups. We encourage our employees to constantly stay abreast of the latest developments and to acquire the highest certifications within security, networks, etc.

Dedicated security and personal data competences

Our security manager is responsible for implementing and maintaining our information security programme. Our internal auditor regularly reviews our security setup and reports directly to management. Finally, we have internal, legal competences within personal data, ensuring that personal data is processed according to the applicable rules both within the company and on behalf of our customers.

Protection of customer data in multiple layers and at several levels

Operational security - Protection of customer data

The main task in our security programme is to take good care of your data. To do this, our security environment is divided into several layers:

- **Physical security**

Our data centres are state-of-the-art and located in Denmark. Therefore, you can be sure that your data remains within the country. Our data centre provider is responsible for the physical environment such as power, cooling, fire suppression and access control, and we carry out stringent checks that our subcontractors always comply with the applicable security regulations for this field.

- **Network**

Our network is segmented, so customers are protected from each other and from threats that move across the network. Next Generation firewalls restrict attacks on customers' environments, and DDoS protection limits the impact a potential attack might have on the servers. Advanced network inspection detects patterns and attack attempts from known malicious IP addresses and alerts our operations department if necessary.

- **Logical access**

We only assign rights to employees who need them and we evaluate them regularly. Only specially privileged employees have access to manage the internal systems.

- **Monitoring**

We monitor our infrastructure and relevant services around the clock. All deviations are registered in our incident management system. In addition to monitoring, we have assigned a 24/7 on-call service.

- **Logging**

We log all access to management and customer environments. In this way, we ensure integrity and traceability and can combine incidents. Our central log platform ensures that we can quickly correlate logs from many sources.

- **Backup**

We perform backup based on the agreed SLA. Backup data is always mirrored between two physically independent locations, so a copy is always available in case of a critical failure.

Emergency and disaster recovery

Preparedness is about being prepared for incidents that may have a critical or disastrous impact on operations. Therefore, we have contingency plans which determine our procedures, routines and roles in the event of a disaster. Employees are trained for such an emergency several times a year.

To secure our technical infrastructure and to spread the risk of critical failure, we use multiple independent data centre providers. We always keep at least one copy of the backup data in a data centre where we do not have production data.

Managing subcontractors

So that we can operate as efficiently as possible, we use subcontractors for selected services. If there is the possibility that the subcontractors may have an impact on our security environment, we ensure that they comply with the same stringent requirements as ourselves. We do this through contracts, data processing agreements, auditor statements, self-regulation and non-disclosure agreements. We regularly check that our subcontractors comply with the requirements.

Audit, compliance and independent third-party assessments

We have a comprehensive compliance programme to ensure that we comply with agreed standards, internal policies and relevant legislation in the field, the purpose of which is to support and safeguard your business:

- **ISO 27001**

ISO 27001 is an international standard for information security management. Several of our competitors claim that they follow the standard, but are not certified. We have been certified since March 2015. The certification must be renewed every year and is audited by both internal and external auditors.

- **ISAE 3402 Type 2**

ISAE 3402 Type 2 describes how we secure the services we provide to our customers, and contains an independent auditor's conclusion on whether the description of our controls are accurate, appropriately designed, and whether the controls have functioned effectively throughout the audited period.

- **PCI DSS 3.2**

Our payment card environment has the highest PCI DSS Level 1 certification, which is renewed annually according to the stringent requirements of the PCI DSS standard from VISA and MasterCard.

- **Penetration testing**

We conduct regular penetration tests on critical components in our infrastructure to see how our systems defend themselves against external threats.

Customers can also perform penetration tests on their own systems following prior arrangement with us.