NorthGRC
CONNECTED COMPLIANCE

Technical White Paper

NorthGRC (formerly Neupart A/S and neupartOne)

1. Security in NorthGRC

This document describes the security design of NorthGRC.

2. Confidentiality, Integrity and Availability

NorthGRC uses Amazon Web Services (AWS) as infrastructure for SaaS. AWS is among the world's largest cloud providers, and many other companies use the Amazon platform. Amazon handles all the infrastructure associated with physical security, such as power, cooling, and internet connections. Amazon offers its AWS hosted in several locations worldwide. However, NorthGRC is only using the Amazon data centers in Frankfurt, Germany.

3. Infrastructure description

3.1. Web servers are hosted on Amazon VPC/EC2 virtual servers with Amazon Linux, .Net, NorthGRC, and neupartOne. Remote management access to servers are limited. HTTP will be redirected to HTTPS, which is the only public allowed protocol into the private cloud zone. The database is a PostgreSQL service hosted within the same private cloud as the application servers, and all access to the database server is limited to this zone. Web servers are using NorthGRC SSL certificates. Amazon provides port level firewalling and filtering services and the Linux based firewall on the web servers allows only SSH, HTTP and HTTPS.

4. Risk assessment

NorthGRC has performed a risk assessment of Amazon as an 'infrastructure-as-a-service' (IaaS) provider. The results were that when compared to other IaaS providers Amazon has

NorthGRC A/S *(formerly Neupart A/S)*
Tobaksvejen 23B, 1st floor, DK-2860 Søborg
Phone: +45 7025 8030
www.northgrc.com

a large financial capability, a large security and operations investment, and because of the large market share, a stronger interest to continue offering secure services.

5. Data Segregation

Each customer is allocated his own separate database.

6. Backup

At least once per day the server makes an image of all data in the database. The backup is encrypted with a customer specific key, before moved to a centralized storage (S3). The daily backups are stored for five years, where they are automatically deleted. On request, NorthGRC can manually delete all backups. The Amazon servers monitor backup jobs and notifies NorthGRC in case of errors. Such notices automatically create a support ticket in NorthGRC's support system. NorthGRC reserves the right to make additional backups of data and store these securely outside of Amazon.

7. Compliance

Despite the physical location of data in Frankfurt (EU), SaaS customers are not to use SaaS to store or process sensitive personal identifiable information. NorthGRC has signed a DPA (Data Processing Agreement) with Amazon.

8. Certifications and Audits

Amazon AWS, including the EC2 services used by NorthGRC, is ISO 27001 certified. ISO 27001 certified companies are subject to recurring internal and external audits. Amazon is also FedRamp and PCI DSS level 1 certified, and subject to SSAE 16 and SCO2 audits. Audit reports are available at Amazon on request. Amazon has mapped its security controls to the Cloud Security Control Matrix and has submitted a publicly available response to the START register of Cloud Security Alliance. Please refer to http://aws.amazon.com/security/ for more information.

NorthGRC A/S *(formerly Neupart A/S)*
Tobaksvejen 23B, 1st floor, DK-2860 Søborg
Phone: +45 7025 8030
www.northgrc.com

9. Availability Zones

NorthGRC is by default not using other availability zones than The Amazon Frankfurt but reserves the right to fail over to other availability zones within the EU (France, Sweden or Ireland).

10. Penetration Test

Recurring vulnerability scans are performed as a part of NorthGRC's ISO 27001 ISMS tasks. Following agreement hereabout, customers can be granted permission to perform their own scans. NorthGRC deliberately selects EC2 machine types which allows external vulnerability scanning. Denial of service test needs to be coordinated with NorthGRC to ensure service capacity for our other customers.

11. Secure Application Design

SaaS is a three-tier application design in which presentation layer, business logic and data layers are physically separated. Thus, the application can only write to the database through the controls provided by the business logic layer. This is protecting SaaS from SQL injection attacks reducing the likelihood of integrity breaches. All three layers are designed to scale depending on the server load. This ensures that the service is always available and responding.

12. Integration

NorthGRC provides Application Programmers Interfaces (APIs) for internal use and to allow integration with other applications. The APIs are used by the NorthGRC frontend to access security, all business logic and database data. The API is only accessible through secure encrypted https and obtained valid security tokens needs to be included in all calls.

The NorthGRC Secure ISMS application uses the API to export a list of selected information in the ISMS application for use in NorthGRC links. The list is exported by request or automatically once every night. The implementation ensures that the integration works on both hosted SaaS versions as well as on-premise installations of

NorthGRC A/S *(formerly Neupart A/S)*
Tobaksvejen 23B, 1st floor, DK-2860 Søborg
Phone: +45 7025 8030
www.northgrc.com

Secure ISMS. The only requirement for using the integration is that the Secure ISMS server is allowed to call the Neupart.one or northgrc.app domain with a secure encrypted https call.

13. NorthGRC staff Secure ISMS access

NorthGRC Support staff cannot login to the NorthGRC instance dedicated to the end customer unless the customer creates and shares login credentials for support purposes. NorthGRC Support staff can create a new User Manager or reset super user account credentials on request from the end customer. All access (including Support staff access) is visible in the activity log

14. Updates

NorthGRC releases NorthGRC updates to SaaS when new versions of NorthGRC become available and when NorthGRC estimates that the new version is relevant for SaaS. Customers can expect at least 4 updates per year. Updates are primarily performed in the standard service window which is Sunday night from 01:00 pm to 02:00 pm CET.

15. Database options

Optionally NorthGRC offers SaaS with non-default database configurations. This SLA does not cover such configurations. NorthGRC recommends that databases are converted to MySQL if it should be used in the SaaS solution.

16. Disclaimer

Amazon offers this SLA to NorthGRC as a basis for their service https://aws.amazon.com/ec2/sla/. NorthGRC can never offer SaaS customers better service or better terms than what Amazon at any time offer and deliver to NorthGRC. NorthGRC offers customers credit for service downtime in SaaS using the same calculation model and conditions that Amazon uses for crediting NorthGRC. NorthGRC's liability is limited according to the End User License Agreement for SaaS.

NorthGRC A/S *(formerly Neupart A/S)*
Tobaksvejen 23B, 1st floor, DK-2860 Søborg
Phone: +45 7025 8030
www.northgrc.com