SLA (Service Level Agreement) for Secure ISMS as a Service

1. SLA for Secure ISMS as a Service

This Service Level Agreement (SLA) describes which services are included in NorthGRC Secure ISMS as a Service (SaaS). This SLA is an addendum to the End User License Agreement for SaaS, as shown in Secure ISMS at first login.

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 the EU.

3. Infrastructure description

3.1. Web servers are hosted on Amazon VPC/EC2 virtual servers with Ubuntu Server LTE, Java, Tomcat and Secure ISMS. Remote management access to servers are limited. HTTP will be redirected to HTTPS, which is the only public allowed protocol. The database is a local installed MySQL service. DNS is using Amazon Route 53. Web servers are using NorthGRC SSL certificates but can be customized with a customer provided certificate. Additional Web server IP address limitation is offered as an option. Amazon provides port level firewalling and filtering services and the Linux based firewall on the web servers allows only SSH, HTTP and HTTPS.

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

4. Risk assessment

NorthGRC has performed a risk assessment of Amazon as an 'infrastructure-as-a-service' (IaaS) provider. The assessment is that compared Amazon to other IaaS providers Amazon has 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 SaaS customers is allocated a separate Amazon EC2 web server instance. The allocated logical Amazon VPC/EC2 server serves as a private server each SaaS customer. This architecture allows NorthGRC to backup and restore a customers' data without impacting data of other customers.

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 Ireland (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.

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

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.

9. Availability Zones

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

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.

11. Secure Application Design

SaaS is a three-tier application design in which presentation layer, business logic and data layers are logically 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.

12. NorthGRC staff Secure ISMS access

NorthGRC support staff cannot login to the Secure ISMS instance dedicated to the end customer unless the customer creates and shares login credentials for support purposes. NorthGRC Support Staff can reset super user account credentials on request from end customer.

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

13. Limited vendor lock-in

The database backup can be restored outside Amazon on a MySQL server. Because the Secure ISMS application is also available as software that installs easily outside of Amazon, the database backup can be used to establish a new Secure ISMS environment outside of Amazon, if so desired. Such a restore requires a valid Secure ISMS license and restore services are not included in the standard SaaS subscription fees.

14. Updates

NorthGRC releases Secure ISMS updates to SaaS when new versions of Secure ISMS become available and when NorthGRC estimates that the new version is relevant for SaaS. 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