NorgesGruppen

Cyber security and NGD suppliers

Version 1.1 23.08.2021

IT og digitale tjenester

NorgesGruppen

1. **Introduction**
   - Cyber Security for suppliers
   - About NorgesGruppen
   - Why Cyber Security is important
   - Expectations
2. **High-level Information Security requirements**
   - Requirements and supplier classification
   - Supplier self-deceleration
3. **Providing vloud services to NorgesGruppen.**
   - Security for cloud providers
   - SaaS security principles

IT og digitale tjenester

NorgesGruppen

Introduction

Cyber security for suppliers

This document is provided to you as a supplier to NorgesGruppen Data to give you an introduction to our security requirements and expectations to you as a supplier, whether you deliver services to NorgesGruppen Data or use our IT infrastructure to deliver services to other companies within the NorgesGruppen group.

Our intention is that by reading this document you will get a high-level introduction into our requirements and expectations with regards to cyber security. Additional and more detailed requirements will be presented as part of purchase process.

The domain of cyber security is no longer only about protecting the local network or the companies' computers and servers. The entry of network connected sensors, cloud solutions and industry 4.0 have made the cyber security domain much wider and complex, where security in the supply chain plays an important role. It is also important to note that cyber security is not only about technical security controls, but also more soft controls, such as policies, risk management and awareness.

The supply chain have become more interconnected and data flows across systems and organizations. Because of this incidents and vulnerabilities in the supply chain willt have an adverse effect on NorgesGruppen and our ability to provide essential services to the public.

Examples of products and services that typically have a cyber security aspect

- Software and hardware
- IoT or IIoT
- Sensors connected to the network
- Cloud based applications and management system (SaaS)
- Industrial Control Systems
- SCADA systems
- Physical Access Control System
- Data analysis services

About NorgesGruppen

This is NorgesGruppen
We take new steps to make tomorrow's retailing less expensive and better, give inspiration for good culinary experiences, and contribute to healthy, green choices.
Our vision is to provide you with a better everyday life. We work hard every day to make sure that the customers choose our stores every time. We shall therefore have the most attractive selection of products, at the lowest possible price. We must make sure that our customers save time and money, have a good food experience, and find it easier to make green and healthy choices.

Our ambitions are to be the customer´s first choice, competitiveness throughout the value chain and sustainable and climate-neutral.

Facts:
- 1,850 grocery stores in 88 per cent of Norway's municipalities
- 900 points of sale as retail convenience goods stores
- 1,000 independent retailers
- 40,000 employees representing 70 different nationalities
- 1,200 business partners

NorgesGruppen IT og Digitale tjenester is the shared service provider for digital services to NorgesGruppen and has been an integral part of the value chain for the entire group since its inception and has played a significant role in the development that has led to NorgesGruppen being today among the country's largest companies.

NorgesGruppen

Why Cyber Security is important

Cyber security is one of our highest priority risks, with breaches and cyber attacks presenting a risk to the security of our information, IT systems and services. We take cyber security very seriously as the threat our digital infrastructure, industrial control systems and our business evolves.

Ensuring a strong and mature state of cyber security in our supply chain is vital to prevent attackers from gaining access to our ICT environment and causing disruption and harm to information systems and our ability to do business and fulfill our social responsibility. We therefore work together with our suppliers to share the role of protecting our information and systems.

How to report a cyber breach or threat to NorgesGruppen

If you suspect it, report it.

If you as our supplier suffer a security breach that impacts NorgesGruppen or you identify a potential risk or threat to our information or ICT systems, you must report it without delay to our Security Operations Centre as well as your usual point of contact within NorgesGruppen.

SOC contact information:
incidentmanagers@norgesgruppen.no
+47 951 21 990 (24/7)

NorgesGruppen

Expectations

NorgesGruppen's Cyber Security expectations to its suppliers

Digital services are becoming more integrated, complex and essential for business, in addition the flow of information often runs across multiple suppliers. Because of this, building and maintaining a healthy supply chain is essential to keep cyber security risk levels down to a minimum.

NorgesGruppen have a set of expectations to our suppliers of digital services that will help improving cyber security posture across the supply chain.

Expectations

1. Comply to laws and legal requirements
2. Have a pro-active approach to cyber security
3. Have an established and functional ISMS
4. Be transparent with NorgesGruppen with regards to security breaches, vulnerabilities and threats.
5. Have effective protocols in place for securing and protecting NorgesGruppen assets and information.
6. Notify NorgesGruppen as soon as possible if you suffer a breach or identify a potential security risk.
7. Provide relevant and updated cyber security training to your staff
8. Challenge us with regards improving our own cyber security posture

NorgesGruppen

Information security requirements

IT og digitale tjenester

NorgesGruppen

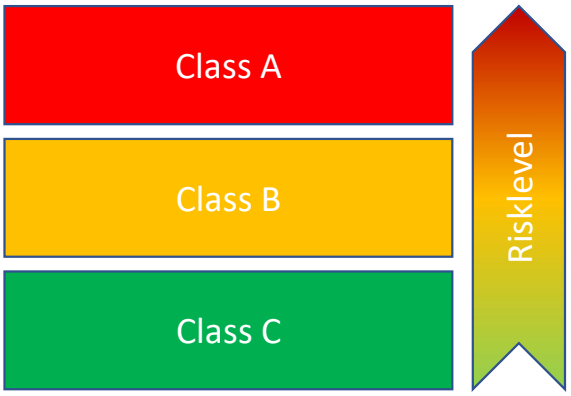
Requirements and supplier classification

Responing to RFI and RFP
When you responds to a request for proposal or information, questions may be asked regarding cyber security controls. These questions will vary according to business area. Please provide as much details as possible as it will speed up the time to assess supplier responses.

Information security requirements are included in supplier contracts. The security requirements in supplier contracts are aligned to the National Institute of Standards & Technology (NIST) cyber security framework, Centre for Internet Security (CIS) and applicable legal requirements. For IoT the ENISA "Baseline Security Recommendations for IoT" is used.

The level of cyber security risk and the supplier's information security footprint within NorgesGruppen, determines the complexity of contractual requirements and the security contract compliance required.

Contract compliance may include an on-site compliance visit, an online assessment, a self-declaration or review of security certifications such as ISO 27001/2 or SOC 1/2. If any security improvement actions are determined, we work with our suppliers to have these remediated as soon as possible.



	Supplier classification
A	Suppliers of services of significant information security footprint for NorgesGruppen. Non-conformities and incidents related to confidentiality, integrity and\or availability impacting the services delivered, can potentially have critical or catastrophic consequences for NorgesGruppen's ability fulfil stated business goals and social responsibility.
B	Suppliers of services with moderate information security footprint for NorgesGruppen. Non-conformities and incidents related to confidentiality, integrity and\or availability impacting the services delivered, can potentially have moderate consequences for NorgesGruppen's ability fulfil stated business goals and social responsibility.
C	Suppliers of services with minor information security footprint for NorgesGruppen. Non-conformities and incidents related to confidentiality, integrity and\or availability impacting the services delivered, can potentially have minor to non consequences for NorgesGruppen's ability fulfil stated business goals and social responsibility.

NorgesGruppen

Supplier self-declaration

Requests for proposal and requests for information

When a supplier responds to a request for proposal or information, you will be asked to submit an “information security self-deceleration”. In addition, questions may be asked regarding cyber security controls.

These questions will vary according to business area. Please provide as much details as possible as it will speed up the time to assess supplier responses.

You should also expect to provide information on

- The products life cycle, security capabilities and program for security updates
- Access management (e.g. User management, SSO support, support for multi factor authentication)
- The use of cryptographic controls for protecting information.
- High level architectural overview of the service offering.

	Information security self-declaration
1	Do you have an information security management system (ISMS), based on recognized standards?
2	In the last 12 months, has the company carried out an audit of its information security management system?
3	Is the management system certified by a third party? - Attach the relevant certificate and the scope of the certification (statement of applicability).
4	Are you in compliance with relevant international and national laws and regulations?
5	Do you have an updated overview of information and equipment associated with the deliveries to NorgesGruppen?
6	Do you have documented routines to ensure that all software and hardware used in the delivery is kept up to date in accordance with the supplier's recommendations?
7	Do you have an established proactive security controls to prevent and detect security breaches that could adversely affect NorgesGruppen?
8	Have all employees and employees who work with information, equipment and services related to NorgesGruppen signed a declaration of confidentiality?
9	Are there life cycle management routines in place to ensure that only authorized personnel will have access to access to NorgesGruppen's IT systems?
10	For remote access to NorgesGruppen's infrastructure, will there be a need to deviate from NorgesGruppen's standard methods of access? (details of our remote access solutions will be made available when/if required)
11	Do you have documented routines for handling security incidents and vulnerabilities?
12	Do you have documented routines for effective notification of security incidents that may affect NorgesGruppen?
13	Are security requirements in the contract made known to and applicable to all subcontractors?
14	Are you, or the your subcontractors, subject to legislation or the subject of a practice by government agencies, which weakens the protection of personal data processed on behalf of NorgesGruppen. Examples of this are legislation that requires the disclosure of personal data to foreign intelligence services or police authorities. If yes, provide detailed answers with reference to relevant legislation.

NorgesGruppen

Providing cloud services to NorgesGruppen

IT og digitale tjenester

Security for cloud providers

Providing Cloud services to NorgesGruppen
Cloud services come in all size and shapes, and can be anything from hosted solutions for industrial control systems and SCADA systems in warehouses and retail stores, to cloud hostsed applications used by the office worker. By providing such services you will process data on behalf of NorgesGruppen and in some cases have access to our IT infrastructure. For these type of services the term SaaS (Software as a Service) is often used

Security testing
To ensure that the provided service is secured and that vulnerabilities are addressed. We require that any SaaS solution provided to us is secured through a programme for penetration testing and risk mitigation.

Secure authentication of users
NorgesGruppen provides a standard identity management platform (Okta) that we expect you as a SaaS provider to integrate with, so our users can use NorgesGruppen standard authentication mechanisms to access your service.

For services that cannot integrate with NorgesGruppen, the provider must use secure and modern methods of authentication. This includes the use of multifactor authentication.

Data processing
You as a SaaS provider, is expected to have full control of any aspect of data processing done on behalf of NorgesGruppen. This is not only limited to personal identifiable information but also includes business information.

Protection of data
Any data in transit must be protected (encrypted) in transit using modern cryptographic controls that are not affected by vulnerabilities and weakness that put NorgesGruppen at risk. For some SaaS services, encryption of data at rest might be also be required.

We also expect that you as a responsible SaaS provider implement the controls necessary to prevent unauthorized access to our data, both from internal and external resources.

Security updates
As a professional provider of a Secure SaaS service, you must make sure that your service are kept up to date with the latest security patches in a seamless manner to all the components of the service.

NorgesGruppen

SaaS security principles

The table below lists SaaS security principles, along with a brief description of its purpose. As a professional SaaS provider vi fully expect you to have taken these principle into consideration as part of securing your service.

	SaaS Security Principles	Description
1	Data-in-transit protection between clients and service	Data should be protected as it transits between the client and the SaaS product. Transport Layer Security (TLS) is a protocol which provides privacy between communicating applications and their users, or between communicating services. When a server and client communicate, well-configured TLS ensures that no third party can eavesdrop or tamper with any message.
2	Industry good practice external certificate configuration	Certificates used within the external TLS connection should follow good practice.
3	Data-in-transit protection between microservices	Data should be protected as it transits between a SaaS provider's microservices. Since microservices can be hosted in different areas of a cloud service, data should be as protected between microservices as it is between client and service.
4	Industry good practice internal certificate configuration	Certificates used within the internal TLS connection should follow good practice.
5	API authentication and protection	All externally exposed API queries which return protected information should require successful authentication before they can be called.
6	Privilege separation	The SaaS product should implement levels of privilege and have authorisation mechanisms in place to enforce the separation of privileges between different types of account.
7	Multi-factor authentication	The SaaS product should implement a method of requiring multi factor authentication to the service. Enabling multi factor authentication helps lower the impact of credential theft.
8	Logging and event collection	The SaaS product generates all relevant security-critical logs.
9	Availability of logs	The SaaS product makes available security-critical events to your audit and monitoring service.
10	Clear incident response to patching and security issues	The SaaS provider has a clearly defined policy for patching internal systems as well as dealing with security issues.
11	Clear and transparent details on a product's security features	The SaaS provider makes available clear and transparent details on the security features that they implement, and how best to configure them

The principles are developed by UK NCSC


Klikk for å legge
til en tittel