NunaGreen
Empowering Green Opportunities

Indaleeqqap 12, kld.
3900 Nuuk
Greenland

IT Policy for External Partners

Requirements and Regulations for Suppliers

Introduction

This IT policy describes the requirements and expectations we have for companies that perform work on our projects. These requirements ensure that all parties protect sensitive data, maintain access control, follow good IT practices, and have reliable backup solutions. Suppliers must be able to document their ongoing compliance with these requirements.

Data Protection Requirements

External suppliers must:

- Ensure that all data is processed and stored in accordance with GDPR (General Data Protection Regulation of the European Union) and other relevant data protection laws.
- Implement technical and organizational measures to protect personal and sensitive information against unauthorized access, loss, destruction, or other unlawful processing.
- Conduct regular risk assessments and security audits to identify and remedy any vulnerabilities.
- Use secure and reliable methods for data transfer, such as encryption, to protect data from unauthorized access.

Access Control to Data

External suppliers must:

- Implement strong access control policies, including the use of unique user IDs, strong passwords, and multi-factor authentication where relevant.
- Restrict access to sensitive data to only those employees who have a legitimate need for access as part of their job responsibilities.
- Log and monitor access to data and systems to quickly identify and respond to suspicious activity.

Good IT Practices

External suppliers must:

- Follow industry best practices and standards for information security and IT management.
- Educate and train employees to follow security procedures and be aware of threats such as phishing and other forms of cyberattacks.
- Establish a security policy that describes how the organization handles and responds to security incidents.

Backup and Recovery

External suppliers must:

- Implement regular backup routines to ensure that all data can be restored in the event of loss or destruction.
- Store backup copies in secure locations and regularly test that backup data can be restored.
- Develop and maintain a disaster recovery plan (DRP) that describes how the organization will restore operations after a major incident.

Documentation and Control

To ensure that suppliers comply with the requirements, they must:

- Prepare and submit documentation upon request that demonstrates compliance with data protection, access control, good IT practices, and backup requirements.
- Participate in audits and inspections ordered by us if necessary to verify compliance with the IT policy.
- Immediately report any security incidents or data breaches and cooperate to mitigate the consequences.

Conclusion

This IT policy is an essential tool to ensure that our external partners protect the data and systems they access in connection with their work for us. By maintaining high standards for data protection, access control, IT practices, and backup, we can minimize the risk of data breaches and other security incidents.

We expect our suppliers to actively collaborate with us to ensure a high level of information security and to continuously document their compliance with the established requirements.

Contractors who have entered into agreements with NunaGreen for a project must ensure that the same IT security standards are included in all agreements with subcontractors on the same project.