

30 June 2025

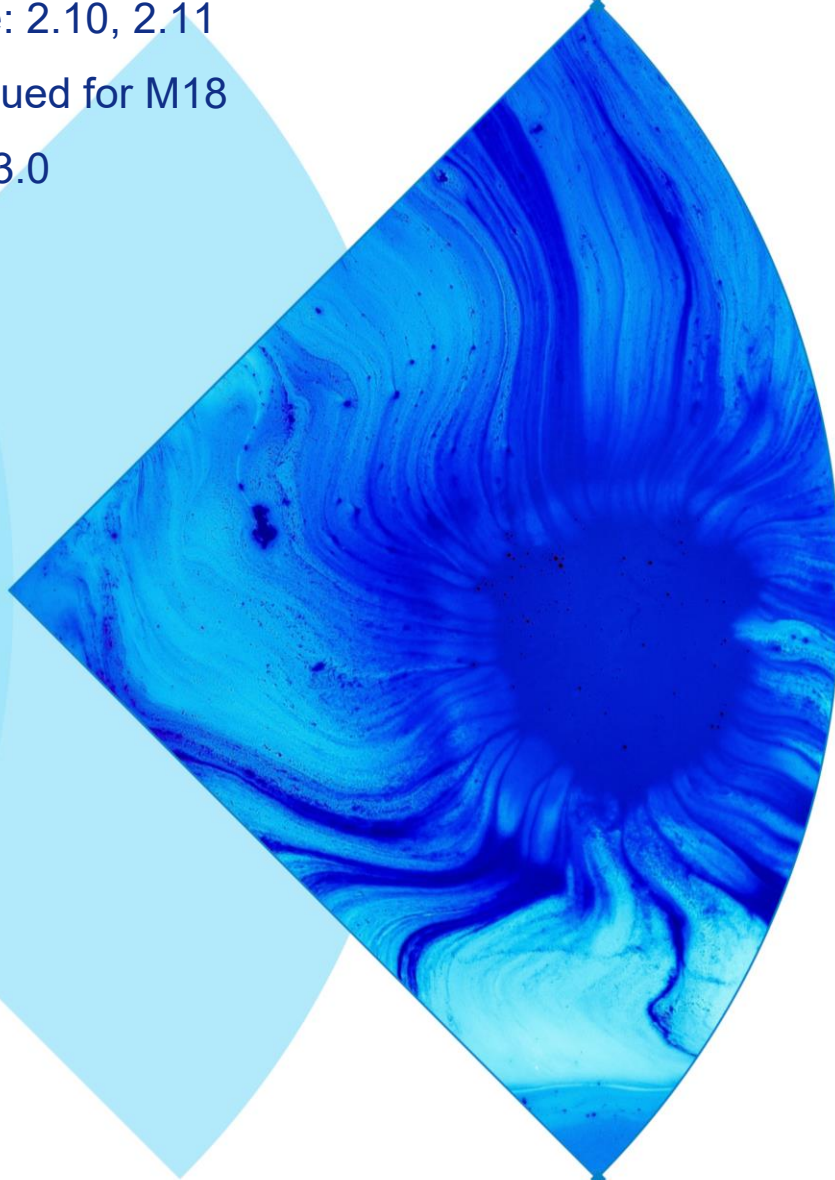
MISD Edge Data Centres

Network Development & Orchestration

Deliverable: 2.10, 2.11

Status: Issued for M18

Version: v3.0



All rights reserved. No part of this publication may be reproduced and / or published by printing, photocopying, microfilm or in any other way without the prior consent of the customer. In case this publication was issued in assignment, all rights and obligations are to be applied following the Dutch DNR 2011, or, should there be an agreement between the parties in question, this agreement applies.

30 June 2025

MISD Edge Data Centres

Network Development & Orchestration

Deliverable: 2.10, 2.11

Status: Issued for M18

Version: v3.0

Author(s)	Azqa Singh <i>Mechanical Engineer</i> Alet-Mari Snyman <i>Process Engineer</i>	07 February 2025	AS
		20 June 2025	AMS
Released by	James Fidgett <i>Project Lead</i>	30 June 2025	JF

Contact person

Azqa Singh
HVAC Engineer
azqa.singh@deerns.com

Deerns Nederland B.V.
Den Haag, Nederland

Content

Version	2
1 Introduction	3
1.1 Background	3
2 Proposed Workflow	4
3 Optimal site criteria	5
3.1 Key Search Parameters	5
3.1.1 Different Network types (mesh or hub & spoke)	5
3.1.2 Sufficient floor area	6
3.1.3 Security	6
3.1.4 Accessibility	11
3.1.5 Maintainability	13
3.1.6 Existing grid issues	14
3.1.7 Proximity to potential waste heat reuse facilities	16
3.1.8 Permissions and due diligence	18
3.2 Tool based solution	19
4 Data sets	20
Annex 1	21

Version

Version	Date	Author(s)	Description
v1.0	07 February 2025	AS	Draft
v2.0	20 June 2025	AMS	Issued for Feedback
V3.0	30 June 2025	AMS	Issued for M18

1 Introduction

1.1 Background

There is increasing interest and need for Edge Data Centres to become a norm within the Netherlands and greater Europe. Due to the lack of space as well as limited availability of power for new developments within the Netherlands, it is crucial to find innovative solutions to keeping up with the growing AI demand. This can be fulfilled by reducing the strain on core/hyperscale DC's and delivering low latency Edge data centres closer to the end users, thus focusing on decentralization.

In order to establish a network of eDC's around the country, the key parameters for an optimal site needs to be defined. This report aims to serve as a framework/decision tree for identifying a suitable site for deployment of an eDC. The next step (v3 and v4 at the next milestone deliverables) would be to create a customizable, interactive tool that incorporates the key search parameters, overlays this on a country-wide map; and is able to identify suitable locations based on user input.

This report is a follow on from Deerns' WP1 reports, the technical feasibility study, which outlines the market research and basis of design to be followed.

2 Proposed Workflow

By leveraging a combination of Geographic Information System tools (GIS), open source data and spatial analysis software, we will be able to identify and filter potential sites graphically. We will need to overlay various data sets to generate a 'suitability map'.

Below is a proposed workflow capturing the steps and tools required to generate the 'optimization tool' for network development:

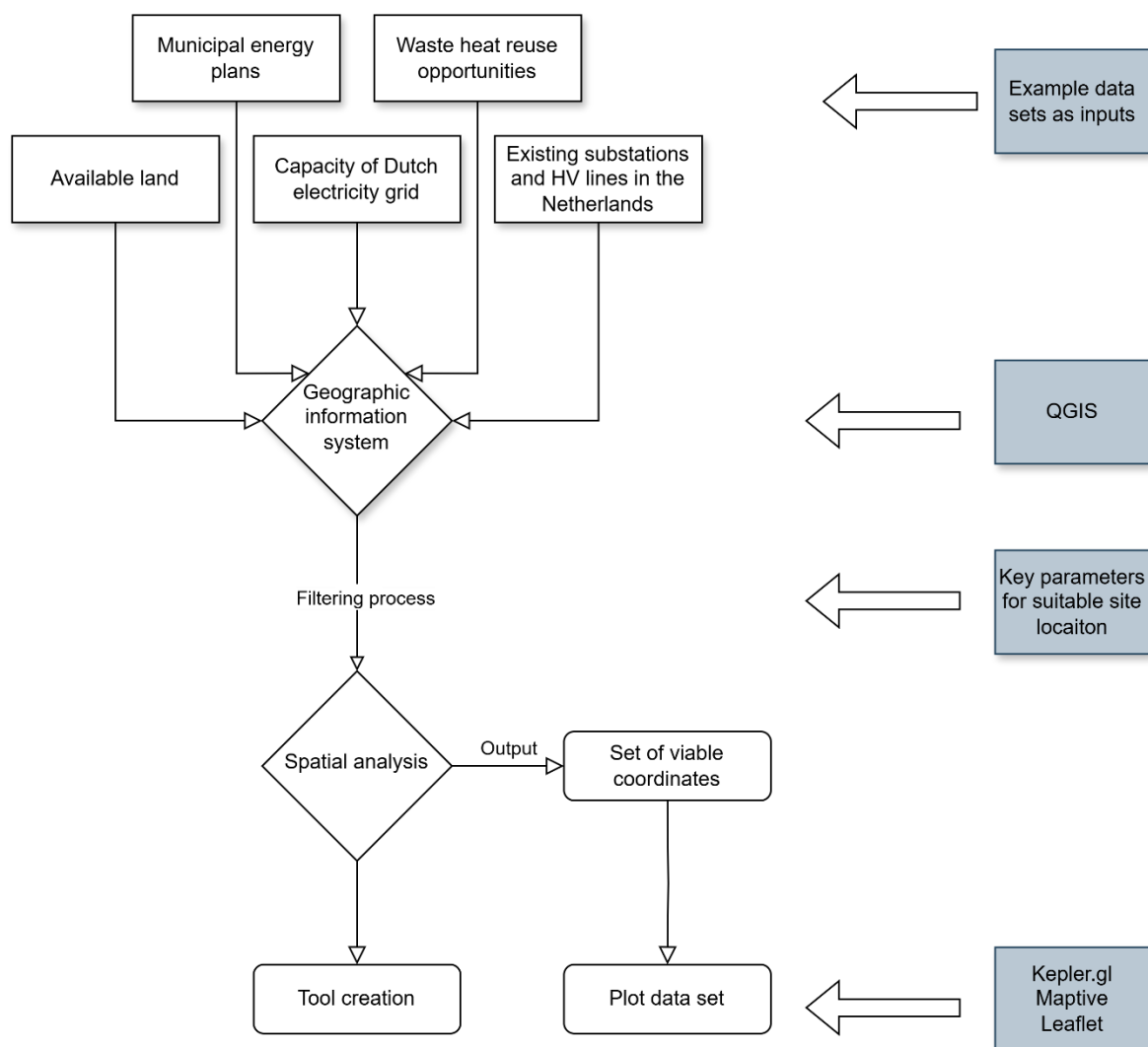


Figure 1: Workflow for optimization tool, Netherlands specific

3 Optimal site criteria

3.1 Key Search Parameters

3.1.1 Different Network types (mesh or hub & spoke)

When deploying edge data centers (eDCs), the choice of network topology significantly impacts performance, resilience, and scalability. Two common models are hub-and-spoke and mesh.

The hub-and-spoke topology connects several peripheral nodes (spokes) to a central node (hub). It's simple, cost-effective, and easy to manage but comes with risks. A failure at the hub can disrupt the whole network, and routing all traffic through the hub can lead to latency and congestion. This model suits centralized data center setups where control is concentrated in one location.

The mesh topology, on the other hand, connects each node to several others, allowing for multiple communication paths. This setup provides high redundancy, fault tolerance, and low latency, making it ideal for applications requiring constant availability and fast response times. For example, a mesh of edge data centers in the Netherlands can offer reliable and fast services locally. If one node fails, nearby nodes can continue operations without disruption. Workloads can also be balanced across the mesh to improve efficiency and responsiveness.

While mesh networks are typically more complex and expensive due to the number of interconnections, this can be managed by using a partial mesh, where only key nodes are directly linked with a scalable design with a few critical interconnections and scale as demand grows. Additionally, software-defined networking (SDN) and automation can simplify management. SDN is a foundational technology for flexible, scalable, and intelligent networks, particularly useful in dynamic environments like edge computing. Edge caching and localized processing reduce unnecessary communication between nodes and decreases latency.

The Netherlands is well-positioned for a mesh-based eDC network due to its dense urban structure, robust digital infrastructure, and focus on sustainability. A mesh can support low-latency applications, improve resilience, and align with data sovereignty and energy-efficiency goals.

In conclusion, while hub-and-spoke offers simplicity, a mesh topology delivers greater resilience and performance which are key benefits for edge data center networks in a highly connected and innovative country like the Netherlands.

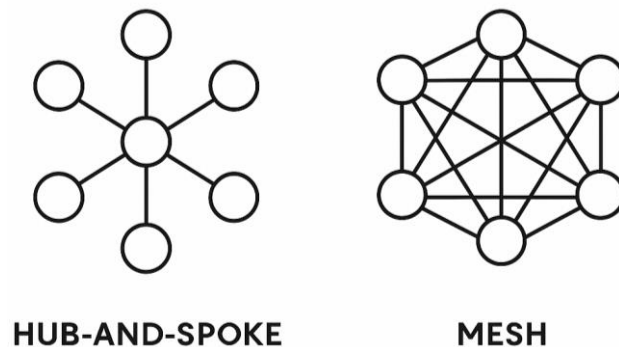


Figure 2: Mesh and Hub-and-Spoke network topologies for edge data centers

The typical distance of edge data centers in a mesh typology:

	Small	Medium	Large
Distance	± 10 km	± 50 km	± 80 to 300 km
Latency	± 2 ms	± 2.5 ms	± 4 ms
Bandwidth	Up to 50 Gb/s	Up to 100 Gb/s	Up to 200 Gb/s
Use cases	Services requiring very low latency, such as real-time applications.	Aggregation of multiple access sites, supporting a broader range of services.	Serving as an aggregation layer for larger capacities and broader coverage.

(Where are edge data centers located, 2021)
(flexential)

3.1.2 Sufficient floor area

The required floor area is a result of the selected cooling system, electrical concept and resilience level. This will be refined and confirmed in the work package 1 design requirements report.

3.1.3 Security

Security is a critical aspect of eDC deployment, encompassing both physical and cyber domains. While cyber security often dominates conversations, physical security plays an equally essential role in ensuring reliability, uptime, and protection from external threats.

The design and deployment of eDC's must include robust physical security measures to ensure resilience against environmental, human, and infrastructural threats. The following key considerations, derived from industry best practices, are particularly relevant for eDC in the Netherlands (TIA, 2020):

1. Environmental Risks:

- **Flooding & Water Protection:** Given the Netherlands' low elevation and proximity to rivers and coastlines, flooding is a critical risk. Site selection must account for flood zones. In the graph below, the green areas on the map indicate that the location is a relatively low-risk area, red and dark red locations are relatively high-risk areas for flooding (see Annex 1).

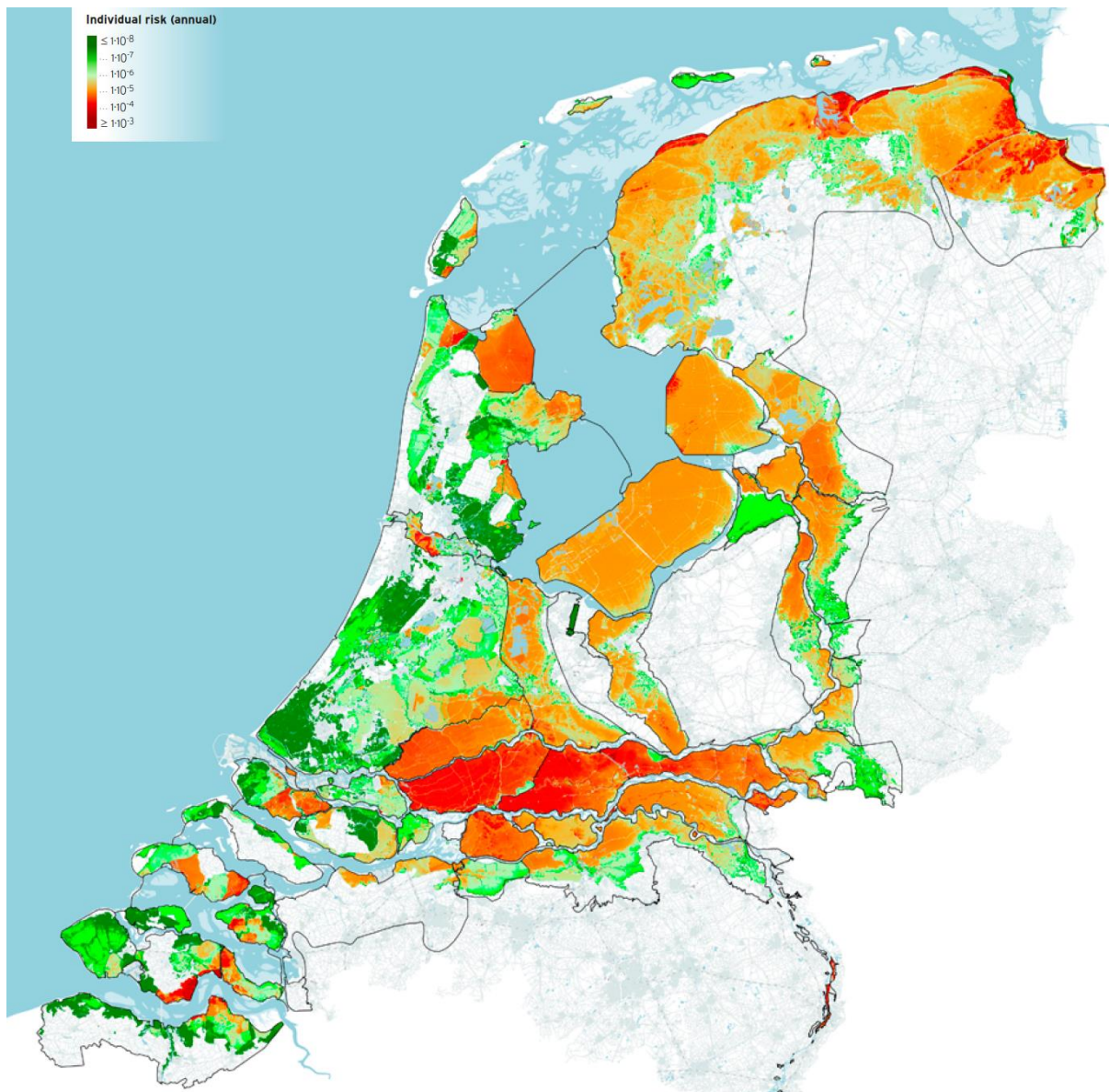


Figure 3: Flood risk map of the Netherlands (Rijkswaterstaat (2017) Flood Risk Map of the Netherlands: Report VNK2. Delft: Rijkswaterstaat, Ministerie van Infrastructuur en Milieu. Available at: <https://repository.tudelft.nl/islandora/object/uuid%3A52035faa-43ab-4dd0-a5b0-099119085356>)



Figure 4: Current probabilities and risks in individual levee systems (Rijkswaterstaat (2017) Flood Risk Map of the Netherlands: Report VNK2. Delft: Rijkswaterstaat, Ministerie van Infrastructuur en Milieu. Available at: <https://repository.tudelft.nl/islandora/object/uuid%3A52035faa-43ab-4dd0-a5b0-099119085356>)

- **Temperature & Humidity:** Extreme temperatures, ranging from -40°C (-40°F) to 60°C (140°F), affect electronics and mechanical equipment. Design should consider that any external equipment supporting the eDC needs to work at the final location conditions. Designers should take into consideration the implications of global climate change that could impact the working conditions of equipment outside of eDC.

The humidity could vary from 0% Relative Humidity (RH) to 100% RH. Most of electronic equipment could support up to 95% RH non-condensing. The issue with low humidity levels is electrostatic discharge (ESD) that it could happen inside EDC and could damage electronic equipment. To avoid ESD risk the humidifier provision could

be an option to analyze ([TIA, 2020](#)). When maintaining a humidity level which is above maintained above 20% RH.

- Wind & Snow Load: Wind load design is crucial in coastal areas, with structural reinforcements for extreme conditions. Snow load compliance should follow Dutch building codes.
- Lightning & Fire Protection: Implement surge protection, grounding systems, fire-rated enclosures, and internal fire detection/suppression systems. To minimize fire risk in environments containing sensitive IT infrastructure, the following protective measures should be implemented, prioritized by impact:
 - Eliminate Flammable Items from IT Areas
 - Avoid storing combustible materials such as paper products, cleaning agents, and similar items near IT hardware. These objects can escalate the chances of a fire and lead to significant downtime.
 - Install Smoke Detection Systems
 - Equip IT spaces with smoke detectors—typically similar to those used in general building areas—to provide early fire warnings.
 - Proper Sprinkler Configuration
 - In spaces without drop ceilings, install upright sprinkler heads. For rooms with suspended ceilings, use concealed sprinkler types to avoid unintentional activation caused by objects like broom handles.
 - Maintain Clearance for Sprinkler Coverage
 - Fire safety regulations often require that sprinkler heads be positioned at least 46 cm (18 inches) above IT equipment to ensure adequate water distribution during fire suppression.
 - Implement Pre-Action Sprinkler Systems
 - Unlike conventional systems that release water upon glass bulb breakage, pre-action sprinklers stay dry until activated by a smoke detection system. This reduces the risk of accidental water discharge.
 - Deploy Cross-Zone Smoke Detection
 - Use a dual-detector approach that only triggers suppression if both detectors sense smoke. This minimizes the possibility of false alarms and unintended system activation.
 - Use Addressable Fire Alarm Panels
 - Equip fire alarm systems with addressable panels that can pinpoint the exact location of a triggered detector, thereby enhancing emergency response times and precision.
 - Incorporate Clean-Agent Fire Suppression Systems

- Opt for suppression agents that do not involve water, as liquid exposure can severely damage IT equipment. Clean agents extinguish fires effectively while protecting hardware integrity.

2. Physical Protection:

To maintain the integrity and security of IT infrastructure, a prioritized approach to physical protection is essential. The following measures are recommended to safeguard access and prevent unauthorized interference (Practical Guide to Ensuring Availability at Edge Computing Sites, Schneider Electric, see Annex 1):

- Secure Access to IT Rooms and Equipment Racks
 - Access to both server rooms and equipment racks must be strictly controlled using locks. Only authorized personnel involved in IT operations or safety functions should have access credentials.
- Door Monitoring Systems
 - Install sensors on all doors associated with critical infrastructure. These sensors should be configured to send alerts whenever a door is opened.
- Power Backup for Security Devices
 - Ensure all physical security equipment remains functional during power outages by connecting them to an uninterruptible power supply (UPS). Devices not located within protected areas might require dedicated UPS units.
- Automatic Alerts for Propped Doors
 - Systems should detect and alert when doors remain open for a specified period, as prolonged exposure increases vulnerability to unauthorized access.
- Surveillance Integration with DCIM
 - Video surveillance systems should be capable of communicating with the Data Center Infrastructure Management (DCIM) system to provide real-time alerts on potential security breaches.
- Motion-Triggered Surveillance
 - Cameras should record footage only when motion is detected or in response to specific environmental triggers. This method conserves storage while allowing rapid identification of incidents, and alerts should be sent via SMS or email to administrators. Remote access via smart devices is also advised.
- Tamper-Resistant Digital Recording
 - Implement network-based color video systems that are resistant to tampering, ensuring data integrity and authenticity of recorded footage.
- Centralized Monitoring Through Building CCTV
 - Integrate the IT area's video surveillance with the main building's CCTV system, allowing security teams to monitor all critical zones cohesively.
- Enclosure Security

- Enclosures must be ruggedized to resist tampering, accidental damage, and weather. Cables and ventilation openings should be protected and hidden.
 - Animal Intrusion Prevention
 - Screens, sealed ingress points, and periodic inspections are essential to prevent damage from wildlife.
 - Perimeter Defenses
 - Use fencing, signage, berms, and surveillance to create a secure boundary. Signage should clearly communicate restricted access.
 - Remote Monitoring
 - Continuous surveillance, access monitoring, and integration with local emergency services are crucial for rapid response.
3. Power Supply Risks
- Ensure dual power feeds and integrate uninterruptible power supplies (UPS) and generators. Consider ASHRAE standards for thermal management, especially in urban or compact deployments.
4. Cabling Security
- Favor underground, armored cables with secure access points and monitored splice locations. Redundant paths should not share the same physical route to avoid simultaneous failure.

5. Video Surveillance

Video surveillance has become an important part of many security solutions, and in the case of EDC security, serves as the first 'layered application' to support Access Control methodologies. A tiered approach for Video Surveillance capability in the context of an Edge Data Center might be represented as below:

- Tier 1: IP-based video surveillance of outside/perimeter with recorded video stored offsite for limited retention period.
- Tier 2: IP-based video surveillance of outside/perimeter, cyber-security protocols manually implemented. Retention period longer than 30 days.
- Tier 3: IP-based video surveillance of both outside and inside of enclosure. Cyber-security protocols to NIST/CIS framework automatically applied. Retention period of 90 days or longer.
- Tier 4: IP-based video surveillance of outside and inside of enclosure, Cyber-security protocols to NIST/CIS framework automatically applied. Yearly testing for vulnerabilities. Retention period of 180 days or longer.

6. Security Metrics

Track KPIs such as video uptime, access logs, firmware status, and breach attempts. Regular assessments and integration with an operations dashboard ensure transparency and responsiveness.

3.1.4 Accessibility

A recent study by the Uptime Institute found that 85% of data center downtime incidents were caused by human error. To mitigate this risk, security must be an integral part of edge data center design, ensuring that only authorized personnel can access IT infrastructure. For instance, IT cabinets should be secured with locks and configured to trigger alerts when accessed without proper authorization.

Additional measures such as biometric access controls and surveillance cameras can further enhance physical security.

On the digital front, it is essential to follow cybersecurity best practices at the edge. This includes careful selection of devices, designing secure network architectures, and ensuring proper setup and configuration of all equipment ([datacenter](#)).

Access Control involves the concerns related to the capability of the eDC to ensure that gaining control to, or of, assets is authorized and restricted based on organizational requirements. Access Control Risk provides the point at which confidential, approved, and authorized eDC physical entry or cyber security supported management is provisioned.

For companies like Microsoft, access control to physical datacenter facilities is tightly controlled by outer and inner perimeters with increasing security at each level, including perimeter fencing, security officers, locked server racks, integrated alarm system, surveillance by the operations center and multi-factor access control. As part of their multi-layered security posture, any unauthorized entry attempts detected by the integrated security systems generate alerts to security personnel for immediate response and remediation ([learn.microsoft.com](#)).

On-site access control include badging systems, biometric authentication, two-factor authentication, access logs. Badging systems are systems where only authorized personnel with valid credentials can enter the facility. Biometric authentication exists out of fingerprint or facial recognition. Two-factor authentication is for higher security, where a combination of smartcard and biometric is implemented. Access logs track all entries and exists that are logged for auditing and forensic investigation.

For unmanned edge data centers, access is often granted temporarily via a secure cloud platform managed by a central NOC (Network Operations Center), 24/7 NOC and 24/7 Service desk. Client Wi-Fi and amenities can be provided ([nlighten](#)).

Remote monitoring and dispatch services offer a scalable and effective solution. By implementing a cloud-based remote service management platform, organizations can continuously monitor conditions at all edge sites, detect anomalies early, and enable rapid response to prevent mechanical failures.

Key Benefits of Remote Data Center Monitoring and Dispatch Services:

- Extended lifespan of critical IT infrastructure
- Lower costs associated with full-time IT management
- Enhanced support for teams with limited resources
- Real-time incident detection and reporting
- Improved visibility into device performance and lifecycle
- Predictive analytics to support proactive contingency planning
- Faster resolution of failures
- Reduced downtime and service interruptions

Modern remote monitoring systems can include integrated sensors for detecting water leaks, temperature changes, as well as surveillance and access control features. These systems generate valuable incident reports and performance data that help teams identify root causes and refine their preventive strategies.

Moreover, this information enables field service engineers to arrive onsite better prepared with the right tools, parts, and a clear remediation plan, reducing repair times and ensuring efficient service delivery.

By deploying digital remote monitoring and dispatch services, organizations can not only safeguard their infrastructure but also reallocate team focus toward strategic activities that drive business value (Best Practices for Edge Data Center Monitoring, Schneider Electric).

3.1.5 Maintainability

Edge data centers are decentralized facilities designed to process data closer to the source, reducing latency and bandwidth usage. Given their distributed nature and often remote locations, maintaining these centers poses unique challenges. Effective maintainability strategies are crucial to ensure operational efficiency, minimize downtime, and extend the lifespan of equipment.

The key benefits of proactive maintenance of data centers are the following (maintenance):

- Minimize Unplanned Downtime
 - Regular maintenance prevents unexpected system failures
- Optimize Performance
 - Consistent monitoring ensures peak technological efficiency
- Protect Business Continuity
 - Stable infrastructure supports uninterrupted operations
- Enhance Security
 - Routine checks identify and mitigate potential technological vulnerabilities

By sticking to a well-structured preventive maintenance schedule, problems can be resolved early, which saves time and costs.

Table 1: Different type of maintenance for edge data centers

Type of Maintenance	Information
Preventive maintenance	Conducting regular inspections and servicing. Key components include: • Uninterruptible Power Supply (UPS) Systems • Power Distribution Units (PDUs) • Heating, Ventilation, and Air Conditioning (HVAC) Systems • Network Cabling
Predictive maintenance	Use of advanced analytics and IoT sensors to predict equipment failures before they happen.
Corrective maintenance	It is maintenance to solve a problem when it occurs. Relying solely on corrective maintenance can lead to higher costs and more downtime. It is better to pair it with preventive and predictive strategies to keep operations running smoothly.

Best practices is also important for data centers. This is where planning and effective strategies plays a role.

Table 2: Best practices to ensure that data centers remain reliable, efficient and secure:

Best practices for maintenance	Information
Develop a comprehensive maintenance plan	Create a thorough maintenance schedule that includes regular inspections, firmware updates,

	and system testing. Consistent check-ups help maintain your equipment and allow you to identify minor issues.
Monitor Environmental Conditions	Proper temperature and humidity levels need to be maintained. ASHRAE (the American Society of Heating, Refrigerating and Air-Conditioning Engineers) recommends keeping data centers within a temperature range of 18°C to 27°C (ASHRAE). Utilize environmental monitoring tools to ensure you stay within these parameters and prevent overheating or moisture-related problems.
Implement Robust Security Measures	Utilize physical and cybersecurity protocols to safeguard the data center.
Regularly Test your equipment	Periodically test generators, UPS units, and other critical equipment to ensure they are ready to operate when necessary.
Partner with Third-Party Maintenance Providers	Collaborating with third-party maintenance providers can be cost-effective while offering specialized support tailored to the requirements.

There are challenges in maintenance which can impact the operations of the edge data center. Aging infrastructure often struggles to meet the demands of modern operations, leading to inefficiencies and compatibility issues comparable to running the latest software on a decade-old computer. At the same time, maintenance costs continue to rise, particularly with Original Equipment Manufacturer (OEM) contracts that frequently involve high expenses and rigid terms, placing additional strain on budgets without compromising on quality. Furthermore, as technology evolves rapidly, organizations face growing challenges in sourcing skilled professionals capable of managing and maintaining increasingly complex systems ([maintenance](#)).

3.1.6 Existing grid issues

The existing power grid in the Netherlands is increasingly congested, making it difficult for new data centres to secure the necessary power supply.

This congestion hampers the industry's growth potential and poses a significant challenge to new and expanding data centres.
([Data center market](#))



Figure 5: Data centres in the Netherlands ([Data Center Map](#))

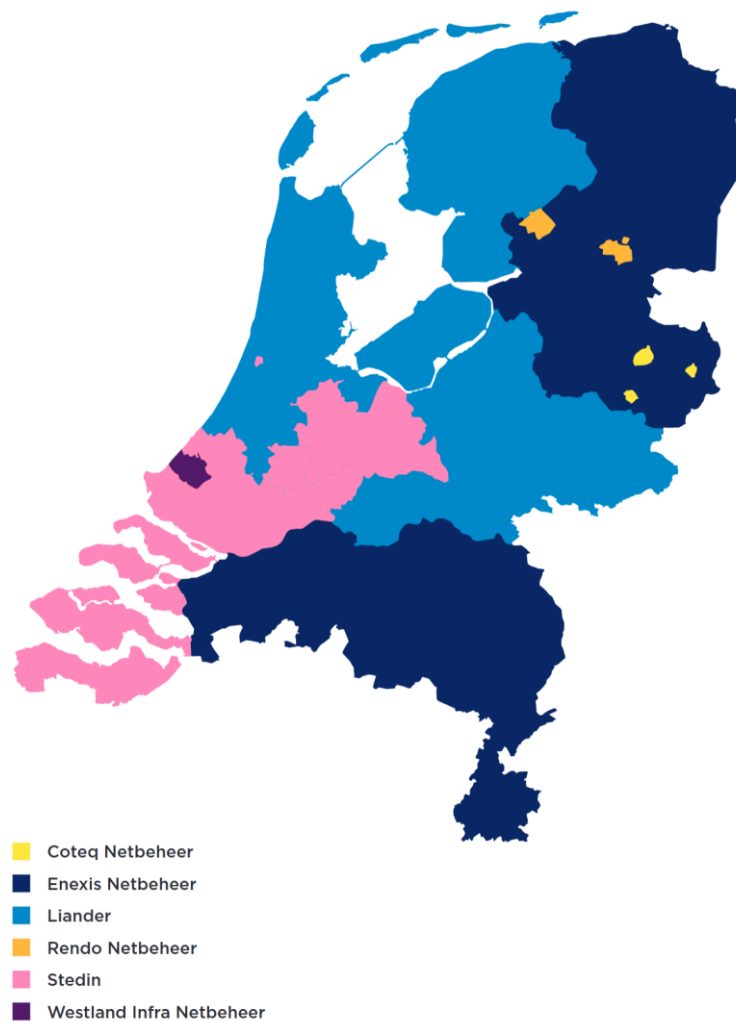


Figure 6: Overview of the regional grid operators ([overzichtskaart-elektriciteit](#)).

3.1.7 Proximity to potential waste heat reuse facilities

In the development of sustainable energy solutions, increasing attention is being paid to the reuse of waste heat as an effective way to reduce energy losses and minimize environmental impact. Edge data centers, which enable decentralized data processing close to end users, represent a promising source of recoverable waste heat. This section explores how the proximity of potential waste heat reuse facilities, close to edge data centers, can influence the feasibility and effectiveness of heat recovery within the project area.

Edge data centers typically generate low-temperature waste heat (20–45°C), which, through heat pumps, can be upgraded for use in residential or commercial district heating networks ([sciencedirect](#)). A number of pioneering projects across the Netherlands illustrate how edge data centers are being co-located near or connected to such facilities:

- Penta Infra's (Haarlem) AMS01 data center is collaborating with heating company Polderwarmte to redirect residual heat into a district heating system serving the Waarderpolder business park. The initiative aims to utilize 100% of the data center's residual heat to warm up the nearby business park ([penta-infra](#)).

- CyrusOne (Amsterdam) is partnering with the Municipality of Haarlem and business park PolanenPark to explore capturing waste heat from its Amsterdam I data center. The feasibility study focuses on enhancing the residual heat and feeding it into a new district heating network to help heat 15,000 homes in the municipality ([cyrusone](#)).
- Smartdc (Rotterdam) supplies residual heat from its data center to the Van Nelle Factory, a UNESCO-listed heritage building. This collaboration demonstrates successful heat reuse in urban and industrial heritage environments ([smartdc](#)).
- QTS (Groningen) is working with WarmteStad, a local utility, to integrate its data center's waste heat into the municipal heating network. The recovered heat is intended to serve thousands of homes in the Groningen area ([data center](#)).
- In cooperation with Vattenfall Heat NL, SilverFalcon (Port of Amsterdam) plans to supply 25 MW of waste heat to the regional heating grid. A high-temperature heat pump (85–120°C) is part of the design to make low-grade data center heat compatible with residential heating ([euroheat](#)).

Below is practical guidelines for typical distance requirements. These are determined from economic viability and heat loss considerations.

Table 3: Heat reuse applications and their typical distance requirements

Application Type	Proximity Requirement	Information	Example	Reference
District Heating	Medium-range (500 m – 5 km)	District heating networks can transport heat over longer distances due to their scale and insulation, but efficiency and cost-effectiveness decrease with distance.	SilverFalcon data center in Amsterdam supplies 25 MW of waste heat to the city's network through a 750 meter pipeline.	Euroheat & Power
Greenhouses	< 1 km (adjacent ideally)	Greenhouses benefit from moderate, steady heating, making co-location or very close proximity ideal to minimize infrastructure needs.	Blockheating supplies heat from modular edge data centers to greenhouses in the Netherlands.	ITRenew and Blockheating
Commercial Buildings	Very close (on-site or adjacent)	For commercial or industrial heating (e.g., office buildings,	The Van Nelle Fabriek in Rotterdam is heated by	Smartdc Rotterdam

		factories), waste heat recovery is most efficient when the user is located next to the data center.	Smartdc's adjacent edge data center.	
Swimming Pools / Sports	Short-range (~1 km)	Pools require constant heating; moderate-temperature waste heat from nearby data centers can significantly reduce gas use. These are often located within neighborhoods; efficiency drops with longer distances.	Die Waterlelie swimming pool in Aalsmeer receives heat from a NorthC data center nearby.	NorthC's Aalsmeer
Domestic Hot Water	Very close (same building or direct pipe)	Domestic hot water (55–60°C) requires higher temperatures or heat pumps, making very short distances essential to avoid energy loss and ensure sanitary standards.		waste-heat-recovery

3.1.8 Permissions and due diligence

The Environmental and Planning Act (Omgewingswet, Ow) is a law for spatial development such as an eDC. One need to comply with this specific law if changes is made to the 'physical environment'. The Environment and Planning Act came into effect on 1 January 2024. The procedure is as follows: a submission of 1 application in one location is made and one decision will be received. Applications will be processed for approximately 8 weeks. For some projects, an [extensive procedure](#) (in Dutch) applies. You will then receive a decision within 6 months ([gov.nl](#)).

Using the Omgevingsloket ([omgevingswet.overheid.nl](#)) enables one to know if you require a permit. Via this online service counter you can:

- Review the [rules per location](#)
- Investigate if environment and planning permit (*omgevingsvergunning*, in Dutch) is necessary ([omgevingswet](#))
- Apply for permits or make reports

- Review information about the quality of the living environment (this possibility will be added to the counter later)

Table 4: Practical process steps to ensure compliance with the Omgevingswet when planning to construct an edge data center in the Netherlands ([Omgevingsloket.nl](https://omgevingsloket.nl), [IPLO.nl](https://iplo.nl)).

Step	Explanation
1. Site Assessment	Verify if location in mind is suitable according to the omgevingsplan/zoning and environmental plan (stibbe).
2. Determine Permit Needs	Use the Omgevingsloket to see which permits (omgevingsvergunningen) are required for the project.
3. Stakeholder engagement	Conduct and document participatory actions
4. Prepare documents	Gather all required documentation: site layout, technical specifications, environmental assessments (if needed), safety plan, etc.
5. Submit Application	File the request for permits or notifications via the Omgevingsloket online portal.

There is also a compensation scheme where a company can receive compensation by the Dutch government if the eDC company is disadvantaged by the Environment and Planning Act and need to the eDC company need to incur extra costs for example the construction project due to a law or a permit.

Energy-saving measures for data centers is outlined in the Recognized List of Measures, which is published on 8 June 2023. This Recognized list of measures encourages energy efficiency and guides organizations in implementing cost-effective measures to reduce energy consumption and greenhouse gas emissions.

Data centre operators are required to consult the Erkende Maatregelenlijst and implement the recognised energy-saving measures that is applicable to their facilities ([data-centre](#)) These measures may include upgrading lighting systems, optimising cooling systems, and implementing advanced power management strategies. Compliance with the Erkende Maatregelenlijst demonstrates a commitment to energy efficiency and helps data centres reduce their environmental footprint ([energiebesparingsplicht](#)).

A specific due diligence need to be carried out once a specific site has been identified.

3.2 Tool based solution

Using a tool like Maptive will allow the user to plot data sets onto a map of the country. This can then be used to identify suitable sites by overlaying all the relevant information and applying filters based on inputs from the 'design requirements' report from WP1.

4 Data sets

To effectively map suitable sites in the Netherlands for building an edge data centre, we'll need access to specific data sets that align with the key parameters that have been defined in the staging and field lab process, as well as general best practices. All of the data sets required for the Netherlands are open source. For wider European projects, a separate workflow will need to be identified.

To be developed further alongside the concept tool development during Milestone 24.

Annex 1

Rijkswaterstaat (2017) Flood Risk Map of the Netherlands: Report VNK2:



vnk-rapport-eng-lr.pdf

Practical Guide to Ensuring Availability at Edge Computing Sites, Schneider Electric:



Schneider Electric -
Practical Guide to Ens

Best Practices for Edge Data Center Monitoring, Schneider Electric



Schneider Electric -
Edge data center.pdf

Deerns Nederland B.V.
Anna van Buerenplein 21F
2595 DA Den Haag
Nederland
+31 88 374 0000
www.deerns.nl

