Complying with NIS2 requirements

Cybersecurity enhancement and business resilience at Priva

PRIVA

Introduction

Priva operates at the intersection of horticulture, indoor growing, and building automation—industries that are increasingly reliant on interconnected systems and digital technologies. As a provider of critical infrastructure and essential services in these domains, we recognize the vital role cybersecurity plays in safeguarding operations and ensuring business resilience for our customers, partners and ourselves. Priva's activities align closely with these criteria. Our solutions underpin essential operations in food production, smart building technologies, and energy management. Disruptions in these areas can have significant consequences, including supply chain interruptions and energy inefficiencies.

We see compliance with the NIS2 Directive as an opportunity to enhance our overall cybersecurity posture. By aligning our operations with this framework, we achieve regulatory compliance while strengthening the reliability and resilience of our solutions. This commitment safeguards our organization and stakeholders, reinforcing Priva's leadership in the horticulture, indoor growing, and building automation sectors.

We are Priva, creating a climate for growth.

Index

04 1. Scope Identification

05 2. Risk Management

07 3. Security Measures and Incident Response

09 4. Continuous Monitoring and Maintenance

10 5. Training and Awareness

11 6. Business Continuity

13 7. Final note

Chapter 1

Scope identification

1.1. Our commitment to NIS2 compliance

At Priva, we recognize the essential role we play in sectors vital to societal and economic stability, such as horticulture, building automation, and indoor growing markets. These industries are increasingly dependent on secure energy systems and digital infrastructure, which are essential to maintaining operational continuity and achieving sustainability goals. The EU's Network and Information Security Directive 2 (NIS2) reinforces the need for robust cybersecurity in these domains, and we are fully committed to aligning with its requirements.

1.2. Building automation: securing smarter, more efficient buildings

Our building automation solutions are designed to optimize energy use, reduce environmental impact, and enhance indoor comfort in commercial and industrial spaces. These systems integrate advanced technologies that connect directly to critical sectors like energy and digital infrastructure. As cyber threats grow more sophisticated, protecting these systems is a top priority. By implementing NIS2-compliant measures, we ensure that our technologies remain secure and operational, safeguarding the trust of our clients and the stability of essential infrastructure.

1.3 Horticulture and Indoor Growing: protecting innovation and sustainability

Priva's solutions are at the heart of modern horticulture and indoor growing markets. Our precision technologies allow growers to control climate, irrigation, and energy use with unmatched accuracy, enabling higher yields and sustainable practices. These systems rely on advanced digital tools and are tightly linked to energy efficiency and food security. By aligning with NIS2, we ensure our innovations remain resilient against cyber risks, protecting food supply chains and advancing global sustainability goals.

1.4 Why compliance with NIS2 is important to us

We view NIS2 as an opportunity to further reinforce our cybersecurity framework and future-proof our operations. We are investing in cutting-edge technologies, robust incident response capabilities, and ongoing employee training to ensure we meet the highest standards of security. By doing so, we not only protect our own systems but also contribute to the security of the industries we serve.

1.5 Our Commitment

By taking a proactive approach to cybersecurity, we aim to remain a reliable, sustainable and innovative partner for the future of the sectors we operate in.

Chapter 2

Risk Management

2.1 Our risk-based approach to cybersecurity

Risk management is at the core of our commitment to safeguarding the security of our network and information systems. As an ISO 27001-certified organization, we have already implemented a robust framework to assess and mitigate cybersecurity risks, ensuring the highest standards of information security and operational resilience.

Our approach begins with conducting regular comprehensive assessments that identify vulnerabilities and potential threats to our systems in the broadest sense. These assessments allow us to gain a clear understanding of the evolving cybersecurity landscape and prioritize actions to address the most critical risks effectively. The ISO 27001 certification reinforces our commitment by requiring a systematic process to evaluate and manage risks, ensuring compliance with internationally recognized standards.

2.1 Technical, operational and organizational measures

To manage risks effectively, Priva employs a multi-faceted approach that includes the following:

1. **Technical measures**: We leverage advanced cybersecurity tools and technologies to protect our network and information systems. This includes implementing firewalls, intrusion detection systems, encryption protocols, and regular software updates to mitigate vulnerabilities.

2. **Operational measures**: Our teams adhere to best practices in operational security, such as routine monitoring of systems, logging and analyzing incidents, and conducting penetration testing on both our internal infrastructure and our customer-facing application. These measures ensure the ongoing integrity and availability of our systems.

3. **Organizational measures**: We have established clear governance structures and policies that define roles and responsibilities for cybersecurity. Regular training programs ensure that our employees are well-equipped to recognize and respond to potential threats and when followed correctly, ensure timely response and mitigation of these threats.

2.2. Cybersecurity risk-based approach alignment with Priva's risk appetite

Through regular reviews and updates to our risk management framework, we stay ahead of emerging threats and continuously improve our defences. This commitment to vigilance and adaptability is a cornerstone of our risk management strategy. We apply this approach not only to cybersecurity but also to broader company-wide risks, supported by the Board of Directors.. Yearly we re-evaluate our current risks and asses if sufficient mitigation has been performed. Only when there is full alignment of the outcome of a particular risk, it will be deemed accepted and mitigated.

Chapter 3

Security measures and incident response

3.1. Incident management

Incident management is a cornerstone of our cybersecurity strategy at Priva, designed to ensure that we can respond quickly and effectively to any security incidents that may arise. Given the dynamic nature of cybersecurity threats, it is essential to have a well-established process in place to detect, manage, and recover from incidents. We have implemented comprehensive procedures that allow us to act swiftly and decisively in response to any security event. Our approach to incident management includes proactive monitoring, clear response protocols, and post-incident analysis.

3.2. Proactive monitoring

An important aspect of our incident management strategy is proactive monitoring. Early detection is crucial in minimizing the impact of any security incident. To this end, Priva leverages monitoring tools and technologies that continuously scan our network, systems, and applications for suspicious activities and potential threats. These tools provide real-time alerts when anomalies or irregular behaviour are detected, enabling our security team to investigate and respond at the earliest stages.

By constantly analysing data for signs of vulnerabilities or policy violations, we can identify threats such as unauthorized access attempts, malware, and other malicious activities before they escalate. This proactive approach helps us address issues before they can cause significant damage or disruption to our operations.

3.3. Clear response protocols

We have a well-defined Security Incident Management Policy that ensures swift, efficient, and consistent action during security incidents. Our response involves assessing the severity of the incident's , containing the threat to prevent further damage, eradicating the root cause, and restoring normal operations. Throughout this process we aim to have transparent communication with internal and external stakeholders .

3.4. Incident reporting

The incident reporting process is streamlined to ensure quick and accurate information flow. Employees are trained to recognize potential incidents and are equipped with clear instructions on how to escalate issues.

Once an incident is detected, it is expected that they report this through our internal reporting channels.

Upon receiving the report, our Security team will assess the situation and activates the appropriate response protocols if the incident is deemed significant. This way, we ensure that relevant external and internal stakeholders are notified when necessary, particularly in cases where the incident may have regulatory or legal implications. We therefore uphold the following deadlines, in accordance with the NIS2 requirements:

Within 24 hours of becoming aware of a significant cybersecurity incident, we notify the Dutch Nationaal Cyber Security Centrum (NCSC). and **after the initial report and within three days,** we will provide follow-up with detailed reports.

3.5. Supply Chain Security

We recognize that cybersecurity extends beyond our own organization to include our suppliers and service providers. To manage supply chain risks effectively, we regularly assess the cybersecurity practices of all external partners. This may include reviewing their security policies, conducting risk assessments, and ensuring they meet our stringent standards. We have established security requirements in contracts and maintain ongoing communication to monitor and manage potential risks. By actively engaging with our supply chain, we ensure that our partners uphold the same high standards of security as ourselves.

3.6. Networking security

Network security is critical to maintaining the integrity of our systems and protecting against unauthorized access. Therefore we have implemented a range of measures to safeguard our networks from internal and external threats. These include advanced firewalls, intrusion detection/prevention systems and virtual private networks (VPNs) for a secure way to enable remote access to our network. We also perform network segmentation, ensuring that data is isolated and protected from unauthorized access. Our team of IT-professionals safeguards this process on a daily basis.

3.7. Access control

To protect our sensitive information and critical systems, Priva has established strict access control protocols. We implemented role-based access controls (RBAC) to ensure that employees and partners only have access to the data and systems necessary for their roles. Access is further secured with multi-factor authentication (MFA), which adds an extra layer of protection against unauthorized entry.

We regularly review and audit user access to ensure that permissions are up to date and reflect each individual's current responsibilities. By maintaining tight control over who can access sensitive information, we reduce the risk of data breaches and unauthorized activities.

3.8. Encryption

Data is safely secured through encryption, both at rest and in transit. All sensitive data stored on our systems is encrypted to prevent unauthorized access, ensuring that even if data is compromised, it remains unreadable.

We also use strong encryption protocols to protect data as it moves across networks, maintaining confidentiality during transmission. Our encryption practices extend to backup systems, ensuring that data remains secure even in the event of a breach. Additionally, we manage encryption keys with strict protocols to safeguard against unauthorized decryption.

Chapter 4

Continuous monitoring and maintenance

4.1 Continuous monitoring: detection of threats

To monitor for threats we employ several monitoring tools and technologies to provide real-time visibility into our network, systems, and applications. Our monitoring infrastructure is designed to detect any suspicious activity, anomalies, or potential threats as soon as they occur. We use a combination of an Security Information and Event Management (SIEM) platform and automated alerting mechanisms to ensure that our security team can quickly identify and respond to potential risks. Our monitoring systems analyze network traffic, suspicious user behaviour, and system logs, allowing us to detect signs of malicious activity, unauthorized access, or data breaches.

4.2 Regular system maintenance

In addition to monitoring, regular system maintenance is essential for ensuring that our IT infrastructure is secure, efficient, and up to date. Though routine system maintenance activities to address performance issues, optimize configurations, and eliminate vulnerabilities. This includes regular patching and updates to both software and hardware components.

By ensuring that all systems, applications, and security tools are up to date, we reduce the risk of exploitation from known vulnerabilities. Our IT team follows a strict patch management process, which includes reviewing and applying security patches promptly as they are released by vendors.

4.3 Updates

We have an update management process in place, through which updates are evaluated, tested, and deployed in a timely manner to minimize the risk of exploitation. We follow large vendor timelines and industry best practices to ensure updates are applied effectively and in alignment with the latest standards.

Chapter 5

Training and awareness

5.1. Security-minded employees

Priva provides regular cybersecurity training sessions for all employees, regardless of their role or seniority and these are mandatory. These sessions cover a wide range of topics, including safe online practices, identifying phishing and social engineering attacks, protecting sensitive data, and understanding the company's security policies and procedures.

In addition, we provide our employees periodic (yearly) refresher courses to keep employees up to date with the latest cyber threats and security practices. These learnings are tailored to address the specific needs and responsibilities of different teams within the organization, ensuring that everyone has the tools they need to protect themselves and the company.

5.2. Awareness campaigns

In addition to formal training sessions, we conduct regular awareness campaigns to reinforce security best practices and keep cybersecurity top of mind for our employees. These campaigns include internal communications such as newsletters, email reminders, posters, and interactive activities. By consistently reminding employees about the importance of cybersecurity, we foster a proactive approach to risk prevention and ensure security remains a key focus."

Chapter 6

Business continuity

6 Emergency procedures

To guide our response efforts, we have developed a comprehensive set of emergency procedures embedded within our business continuity plan. This plan incorporates various policies, such as our Security Incident Management Policy, Crisis Communication Protocol, and Cloud Incident Protocol, ensuring that we are well-prepared for a range of scenarios that could impact our operations.

When a security incident is detected, whether it's a cyberattack, system failure, or cloud service disruption, our emergency procedures are activated immediately. These procedures provide clear, step-by-step actions to minimize damage, safeguard critical assets, and ensure a swift, coordinated response across the organization. The response plan includes securing affected systems, isolating the threat, and engaging with key stakeholders to deliver transparent updates throughout the situation.

In the event of a cloud-related incident, our Cloud Incident Protocol ensures prompt actions to secure data, resolve service outages, and collaboration with cloud service providers for a resolution.

Our Crisis Communication Protocol ensures that all internal and external communications are handled with accuracy and transparency, providing critical updates to employees, regulators, and other stakeholders. For our customers we have setup portals through which we can communicate quickly and efficiently and provide updates when necessary.

Each of these protocols triggers a distinct response that aligns with the type of incident, allowing our teams to respond quickly and efficiently.

Our business continuity plan accounts for a range of potential crises, ensuring we are prepared for various scenarios. Through simulated crisis exercises, we equip employees to respond confidently and effectively under pressure, minimizing confusion or delays

6.1. Rapid system recovery

A key element of our business continuity plan is ensuring the rapid recovery of critical systems and data following an incident. We maintain current backups of essential systems and information, enabling us to restore services quickly and minimize downtime in the event of a cyberattack or system failure..
Our disaster recovery procedures prioritize the swift restoration of critical infrastructure,

including network access, data storage, and application services, to ensure business operations resume without delay. This strategy is supported by close collaboration with our trusted cloud service providers, leveraging their scalable infrastructure and expertise. These partnerships are vital to maintaining resilience, offering the reliability and capacity needed to support seamless recovery efforts. .

Our recovery processes are regularly tested through simulated exercises to ensure their effectiveness. This allows us to identify potential weaknesses in our plan and refine our approach to system restoration.

Final note

At Priva, cybersecurity and business continuity are top priorities, and we are committed to maintaining the highest standards to protect our systems, data, and operations. Through comprehensive incident management procedures, proactive monitoring, continuous employee training, and robust controls we ensure that we are prepared for a wide range of potential cybersecurity threats and challenges.

We maintain a proactive approach to cybersecurity, continuously improving our strategies to address emerging risks and safeguard the integrity of our infrastructure. Our detailed business continuity plan ensures that, in the event of a major incident, we can respond quickly and efficiently to minimize impact and maintain operations.

For any further inquiries or detailed information regarding the policies and processes outlined in this document, please do not hesitate to contact your Priva representative. We are dedicated to ensuring a secure and resilient environment for all our stakeholders.