Information Security

NIS2 Directive

Disclaimer
This document is prepared by Bühler AG. Bühler AG acts in its function as an independent third party, but nothing in this document should be read or purported that Bühler AG may be acting as an expert.

This document outlines Bühler's view on the NIS2 Directive, a new European Union (EU) legislation enhancing cybersecurity requirements for entities across the EU. It details the directive's key requirements and describes how Bühler is aligning its cybersecurity practices to meet these standards. The focus of the NIS2 is on implementing robust risk management strategies, ensuring timely incident reporting, and maintaining compliance with the directive's comprehensive security and reporting obligations.

About the NIS2

The NIS2 (Directive (EU) 2022/2555) is a significant step forward in strengthening cybersecurity across the European Union, expanding the scope of its predecessor NIS to include a broader range of sectors and companies. It imposes obligations on both essential and important entities - it is estimated that 160,000 companies will be affected by NIS2. These obligations include implementing robust risk management practices, mandatory incident reporting, ensuring supply chain security, and adherence to stringent compliance and oversight mechanisms. The directive emphasizes the need for enhanced collaboration in information sharing, both within member states and across borders, to bolster collective cyber resilience. With stricter penalties for non-compliance, NIS2 demands a proactive and comprehensive approach to cybersecurity, reflecting the EU's commitment to safeguarding its digital economy and infrastructure against escalating cyber threats.

Scope of the NIS2

NIS2 applies to all companies falling into two main categories: Essential Entities (EE) and Important Entities (IE). NIS2 applies to Bühler as an Important Entity for Manufacturing.

Essential Entities (EE)	Important Entities (IE)
Size threshold: varies by sector, but generally 250 employees, annual turnover of EUR 50 million or balance sheet of EUR43 million. • Energy • Transport • Finance • Public Administration • Health • Space • Water supply • Digital Infrastructure (e.g. cloud computing providers)	Size threshold: varies by sector, but generally 50 employees, annual turnover of EUR 10 million or balance sheet of EUR 10 million. • Postal Services • Waste Management • Chemicals • Research • Foods • Manufacturing • Digital Providers (e.g. social networks, search engines, online marketplaces) Plus all sectors under Essential Entities and within the size threshold for Important Entities.

Penalties

Noncompliance with the NIS2 can be sanctioned with fines as well as sanctions for the management.

Fines

Essential Entities: EUR 10 million or 2% of global annual revenue, whichever is higher.

Important Entities: EUR 7 million or 1.4% of global annual revenue, whichever is higher.

Sanctions for management

NIS2 allows authorities to hold organization managers personally liable if gross negligence is proven after a cyber incident. This includes:

- Ordering organizations to make compliance violations public.
- Making public statements identifying the natural and legal person(s) responsible for the violation and its nature.

- If the organization is an Essential Entity, temporarily ban an individual from holding management positions in case of repeated violations.

Requirements of the NIS2

The NIS2 covers four primary areas to strengthen a company's cybersecurity resilience to withstand cyberthreats.

Management	Reporting to authorities
Management must be aware of the directive's requirements and risk management practices. They are primary responsible to identify and mitigate cyber risks to ensure compliance with the directive.	Organizations must set up processes to ensure prompt reporting to authorities, such as the mandate to report major incidents within 24 hours.
Risk management	**Business continuity**
To meet the new requirements, organizations must implement measures to minimize risks and consequences. This includes incident management, improved supply chain security, network security, access control, and encryption.	Organizations must consider how to ensure business continuity in case of major cyber incidents. This includes, for example, system recovery, emergency procedures, and establishment of a crisis response team.

Minimum measures

At Bühler, we understand the importance of cybersecurity in today's interconnected digital landscape. As an ISO 27001 certified company, we have implemented the NIS2 standards, with a specific focus on customer's duties to secure their supply chain. Not all requirements of the NIS2 directive apply equally to businesses and organizations. They vary based on the business size, societal role, and exposure level to ensure proportionality and prevent smaller businesses from undue impact. Some minimum measures are mandatory for all relevant entities. Below you can find a list of the minimum requirements of the NIS2 directive and how Bühler addresses them.

NIS2 minimum measures	How Bühler addresses the requirement
Risk assessments and security policies for information systems.	Bühler maintains a framework of security policies and procedures as part of the Information Security Management System (ISMS) to conduct risk assessments to identify and address information security risks.
Policies and procedures for evaluating the effectiveness of security measures.	Bühler has established an internal audit program to ensure the effectiveness of all security controls managed by the ISMS. External certification audits are conducted to assess the compliance with the ISO 27001 standard. Nonconformities identified during these audits are addressed through a defined corrective action process.
Policies and procedures for the use of cryptography and, when relevant, encryption.	The legal and required use of cryptography, such as encryption at rest or in transit, is defined in the security policy framework. For example, all employee computers or corporate-managed smartphones have full-disk encryption enabled.
A plan for handling security incidents.	Bühler maintains an emergency organization, processes, and procedures to handle and respond to security incidents. This includes, as required, the communication with external parties such as authorities and customers.
Security around the procurement of systems and the development and operation of systems. This means having policies for handling and reporting vulnerabilities.	The security policy includes requirements for the procurement and development of IT systems and applications. This includes requirements for dealing identified vulnerabilities.
Cybersecurity training and a practice for basic computer hygiene.	All Bühler employees must complete multiple information security trainings as part of their onboarding process. Specifically about the risk of phishing and social engineering, all employees receive ongoing training (multiple times a month) in the form of simulated phishing attacks and micro-trainings.

Security procedures for employees with access to sensitive or important data, including policies for data access. The company must also have an overview of all relevant assets and ensure that they are properly utilized and handled.	Security policies define the acceptable use of IT systems and data based on their (confidentiality) classification. A global asset management system is used to inventory all relevant IT systems and "information repositories", critical third-party suppliers, etc.
A plan for managing business operations during and after a security incident. This means that backups must be up to date. There must also be a plan for ensuring access to IT systems and their operating functions during and after a security incident.	Bühler maintains a business continuity management framework to ensure that the defined business processes can be securely resumed in case of an incident. The respective recovery plans undergo recurring reviews and tests.
The use of multi-factor authentication, continuous authentication solutions, voice, video, and text encryption, and encrypted internal emergency communication, when appropriate.	Security policies define in what access scenarios a system or application requires multi-factor authentication and its events are continuously monitored. The business continuity management framework and emergency organization define the secure communication channels to be used in case of an incident.
Security around supply chains and the relationship between the company and direct supplier. Companies must choose security measures that fit the vulnerabilities of each direct supplier. And then companies must assess the overall security level for all suppliers.	The security requirements for third parties such as suppliers are defined. Applicable third parties must confirm their compliance with the security requirements with an amendment as part of the overall contract and business relationship with Bühler. Furthermore relevant suppliers undergo recurring audits and need to confirm their maturity in cyber risk management and business continuity.
Essential and important entities must have processes in place for prompt reporting of security incidents with significant impact on their service provision or recipients. NIS2 sets specific notification deadlines, such as a 24-hour "early warning".	The defined security incident management process includes the parties to be notified and the associated notification times. This includes the required reporting as defined by NIS2. Similarly, the reporting requirements for data protection laws such as the EU General Data Protection Regulation (GDPR) are defined.

These descriptions are general summaries of the areas covered by the NIS2 directive and are therefore not fully comprehensive. To ensure that your specific company complies with the NIS2, we highly recommend seeking advice from an expert.

Security of Bühler products and services

Digital platforms such as **Bühler Insights, myBühler** or **Mercury MES** are developed and maintained according to a defined secure development lifecycle based on IEC62443-4-1. This means that security considerations are incorporated into all phases of the software development process, including threat modeling to identify security risks, performing security testing activities and following corporate security requirements, and responding to emerging security risks after release, such as providing patches for vulnerabilities.

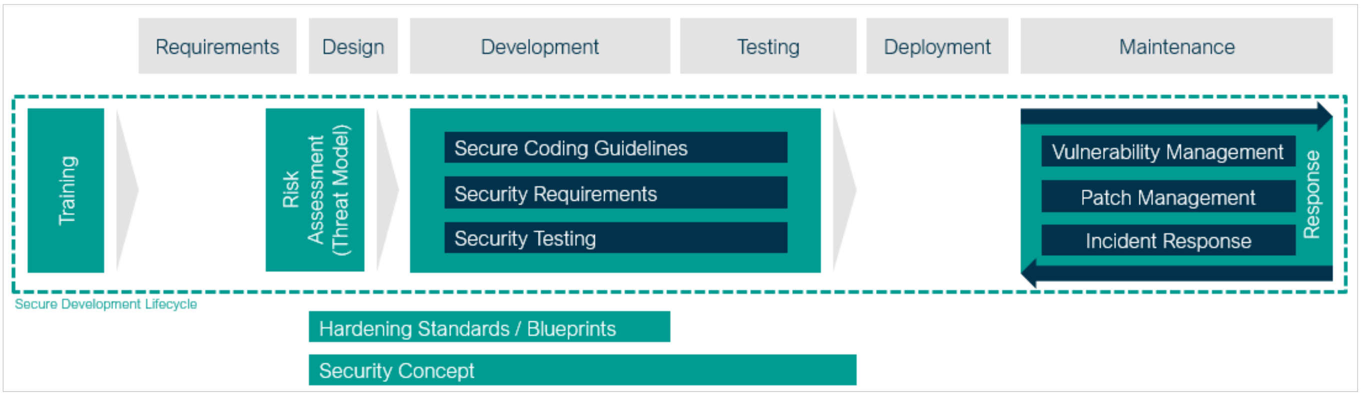

Figure 1 Secure Development Lifecycle

Bühler digital platforms comply with the NIS2 requirements such as encryption, secure development, user access management and multi-factor authentication. For more information, please contact your sales representative or use the contact form.

References and further information

- NIS2 (Directive (EU) 2022/2555) on EUR-Lex
- Information Security at Bühler on www.buhlergroup.com

Disclaimer

This document is not part of and/or subject to the agreement regulating the use of the services or any purchase. The information in this document is not a commitment, promise, or legal obligation to deliver any material or service or to develop and provide any specific security feature or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of their dates, and they should not be relied upon in making purchasing decisions. This document is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. Bühler assumes no responsibility for errors or omissions in this document. As a consequence we will not be liable to you or any other third party in respect of business losses, damages, expenses, commercial opportunities or goodwill arising out of or in connection with this document.

Bühler Group
Gupfenstrasse 5
9240 Uzwil
Switzerland

www.buhlergroup.com

v1.0, June 2024