

General cybersecurity requirements for suppliers cooperating with Polpharma

At Polpharma, we attach particular importance to **the security of information, systems and business continuity**. That is why we establish cooperation with business partners and technology service providers who meet legal requirements in this area and operate in accordance with recognized standards and good cybersecurity practices.

What are our requirements?

1. Suppliers should ensure that their operations comply with applicable cybersecurity regulations, including the NIS2 Directive and national legislation implementing these requirements, where applicable to their operations. As an essential entity under these regulations, we expect suppliers to adopt an approach appropriate to the requirements of working with such an entity, particularly by being ready to share security-related information.

Even if a given supplier is not formally covered by these regulations, we pay attention to adapting processes and security measures to their requirements. Such an approach supports the construction of a resilient and secure supply chain and can be an important element of assessing the ability to cooperate with Polpharma.

2. Processes related to cybersecurity should be based on widely recognized standards and frameworks, such as:

- ISO/IEC 27001 and related ISO 27000 family standards,
- NIST Cybersecurity Framework (CSF),
- CIS Controls,
- OWASP (in the field of application security),
- other equivalent industry or regulatory standards appropriate to the nature of the services provided.

3. Based on legal requirements and applicable standards, suppliers should implement appropriate organisational and technical measures to ensure, in particular:

- protection of information and data, including - personal data,
- cybersecurity risk management,
- access control,
- security monitoring and
- effective management of vulnerabilities and incidents, including early and direct notification in the event of exposure of Polpharma's data or access to additional risks related to an incident or threat.

4. We stipulate that in each case in which we wish to establish cooperation with a supplier, we may:

- provide detailed requirements, adapted to the type of cooperation,
- verify that the supplier has met these requirements. In particular, we may ask additional questions, ask for documents, certificates, audit results or arrange for an audit of the supplier.

Access rules

If we establish cooperation that requires access to our ICT resources, such access can only be carried out through a corporate Privileged Access Management / Privileged Identity Management (PAM/PIM) system.

We don't allow alternative remote access methods that don't take into account the governance, authentication, and logging mechanisms provided by this solution.