Antibiotice

Cyber Security Policy

2024

In the context of sustainable development, Antibiotice SA considers cybersecurity an essential component of corporate governance, of the protection of stakeholders' rights and of the operational continuity. Computing and communications resources are managed responsibly, in accordance with legislation, international standards and internal policies, thus contributing to ethical, secure and sustainable activity.

1. Purpose of the policy

Cyber Security Policy sets out the framework that defines the rules and measures necessary to protect computing and communications resources of Antibiotice SA. The policy ensures the information confidentiality, integrity and availability protection, contributing to:

- preventing the digital risks with economic, social and reputational impact;
- protecting the rights and personal data of employees, customers and partners;
- ensuring a resilient and sustainable IT infrastructure.

2. Integrated ESG principles

- Confidentiality: protecting personal data and sensitive commercial information;
- Integrity: promoting an ethical behavior when using technology. Preventing unauthorized modification or destruction of information;
- Availability: ensuring the continuity of essential economic activities under conditions of transparency and accountability.

3. Applicability and commitment

The policy applies to all employees, collaborators and suppliers who create, store, access or transmit data and information using the Antibiotice infrastructure, encouraging ethical and responsible behavior in the digital environment.
The document is communicated transparently and is part of our commitments to ESG (Environmental, Social, Governance) criteria.

4. Organizational responsibility

- Cyber Security Team: acts proactively to prevent risks and ensure a sustainable IT infrastructure.
- Incident Response Team (IRT): intervenes and handles security incidents efficiently and transparently to ensure the continuity of critical activities. The team activates the business continuity plan in crisis situations.

5. Digital rights protection, training and awareness

The company complies with the data protection legislation and ensures a secure digital working environment, by:

- monitoring access to data and systems;
- informing the employees about their digital rights as well as their obligations to comply with security policies and procedures;
- regular training for employees on cyber risks, responsible use of technology and data protection.

6. Use of electronic communications

Email and internet are used exclusively for professional purposes. The activities are monitored to prevent the cyber risks.

7. Security incident reporting

Any incident (unauthorized access attempt, data loss, etc.) must be reported immediately to the direct hierarchical boss or the IT security team.

8. Confidential data transfer

• Confidential data must be protected and disclosed only according to the internal procedures.

9. Information classification

The information is classified as follows:
• public;
• internal;
• confidential;
• with limited access.

10. Physical security

Access to IT equipment and sensitive areas is controlled through the access cards, video surveillance systems and strict authorizations.

11. Remote work

Employees working remotely must comply with the same security measures as those working within the company headquarters.

12. Change management

Any change made to the IT infrastructure is documented, tested and approved according to a controlled process.

13. Systems auditing

Periodic audits are performed to assess compliance and identify vulnerabilities.

14. Disaster contingency plan

This plan includes backup procedures, data restoration testing, and scenarios for maintaining business in crisis situations.

15. Training and awareness

Employees participate in regular training sessions on cybersecurity and best practices.

16. Sanctions policy

Violation of the policy provisions will result in disciplinary sanctions, which may include termination of the employment contract.

17. Incident management

Clear procedures are in place to document, investigate and remediate security incidents in order to prevent their recurrence.

18. Value chain and suppliers

Partners and suppliers are encouraged to adopt similar cybersecurity standards and to comply with data protection requirements.

19. Review and update

The policy is reviewed annually and whenever relevant legislative or technological changes occur, to reflect the ongoing commitment to sustainability and compliance.

20. Reporting violations

Antibiotice SA encourages the reporting of any situations that contravene the principles and provisions of this Cybersecurity Policy. Any notification regarding the non-compliance with this policy can be transmitted through the following channels:

- directly to the **hierarchical superior**, in the case of employees;
- to the **Incident Response Team** via this contact form on the site.

All the complaints are reviewed in accordance with the internal incident management procedures and are handled promptly, fairly and professionally.

Antibiotice a+