

**Westward Way Tech N.V.**



**Data & Cybersecurity Measures**

2025

# **Content**

- 1. Data Protection & Governance**
- 2. Access Control & Security**
- 3. Encryption & System Safeguards**
- 4. Monitoring & Incident Response**

# **1. Data Protection & Governance**

The company recognizes data as a critical asset and applies structured governance to ensure its confidentiality, integrity, and availability. Sensitive information, including customer identity records, financial data, and internal operational files, is classified according to defined risk levels. Ownership and accountability for each category of data are clearly assigned, ensuring that responsibilities for protection and usage are transparent across the organization.

## **2. Access Control & Security**

Access to company systems and data is restricted on the principle of least privilege. Employees and contractors are granted only the level of access necessary to perform their duties. Strong authentication measures, such as multi-factor authentication (MFA), are enforced across critical systems. Access rights are reviewed regularly, and inactive or unnecessary accounts are promptly removed to reduce exposure to unauthorized use.

## **3. Encryption & System Safeguards**

All sensitive data is protected by encryption both in transit and at rest, ensuring that information remains secure during transfer and storage. Secure storage solutions and robust backup mechanisms support data recovery in the event of system failure or incident. Systems are maintained with regular security patching, vulnerability assessments, and adherence to secure configuration standards, minimizing the risk of exploitation.

## **4. Monitoring & Incident Response**

The company operates continuous monitoring of networks and critical systems, supported by logging and alerting mechanisms that can identify unusual or unauthorized activity. An incident response framework is established, with defined roles, escalation paths, and communication protocols. In the event of a confirmed data breach, timely notification to regulators, affected customers, and other stakeholders will be made in accordance with legal and contractual obligations.