Brytend B.V.
Thorbeckelaan 152
3362 WV SLIEDRECHT
The Netherlands
+31 (0) 85 013 02 04
info@brytend.eu
www.brytend.eu

IT Security Policy.

Date: 01-04-2024.

Purpose

The purpose of this IT Security Policy is to protect the integrity, confidentiality, and availability of Brytend B.V.'s information technology assets and data.

Scope

This policy applies to all employees, contractors, and partners of Brytend B.V., including all hardware, software, and data owned or used by Brytend B.V.

Policy Statement

Brytend B.V. commits to maintaining a secure and reliable IT environment to support the delivery of its SaaS solutions to partners.

General Principles

Data Protection: All data must be classified and handled according to its classification level.

Access Control: Access to systems and data is granted on a least privilege basis.

User Responsibility: Users are responsible for the security of their credentials and devices.

Security Measures

Firewalls and Antivirus: Adequate firewalls and antivirus software must be installed and regularly updated on all systems.

Encryption: Data in transit and at rest must be encrypted.

Patch Management: Regular updates and patches must be applied to all software and systems.

Incident Response

Reporting: All security incidents must be reported immediately to the IT Security Team.

Analysis: Incidents will be analysed to determine their cause and impact.

Resolution: Steps will be taken to resolve the incident and prevent recurrence.

Compliance

Legal and Regulatory: Brytend B.V. will comply with all applicable legal and regulatory requirements regarding cybersecurity.

Audits: Regular internal and external audits will be conducted to ensure compliance with this policy.

Training

Awareness: All staff will receive regular training on IT security best practices and this policy.

Phishing: Staff will be trained to recognize and respond to phishing attempts.

Physical Security

Access: Physical access to critical IT infrastructure is restricted.

Surveillance: Surveillance measures are in place to monitor access to sensitive areas.

Remote Work

VPN: Remote access to the network must be done through a secure VPN.

Device Security: Devices used for remote work must meet Brytend B.V.'s security standards.

Policy Enforcement

Violations: Violations of this policy may result in disciplinary action, up to and including termination.

Review and Update: This policy will be reviewed annually and updated as necessary.

Acknowledgement

All employees, contractors, and partners must acknowledge that they have read and understood this IT Security Policy.