SECURITY POLICY SUPPLIERS

VDL GROEP

VERSION 1.0

STRENGTH THROUGH COOPERATION

INTRODUCTION

In today's digital world, information security is crucial for protecting company data and ensuring the continuity of our operations. VDL strives to ensure information security in all its processes and expects the same from its suppliers. This security policy has been drafted to outline clear guidelines and expectations regarding the security measures to be implemented and adhered to by its suppliers.

The purpose of this policy is to create shared responsibility for protecting sensitive information and to ensure that all parties involved are aware of their role in maintaining secure and reliable cooperation. VDL values cooperation with our suppliers and believes that by adhering to these guidelines, together we can create a safe and resilient working environment.

Confidentiality level	Public
Scope	VDL Groep
Version	Version 1.0
Print version date	11/12/2024
Author	Security Office
Department	VDL ICT Security

CONTENTS

2 POLICY ARTICLES

2.1 GENERAL TERMS AND CONDITIONS

The Supplier shall comply with all applicable laws and regulations, including but not limited to the GDPR, DORA, NIS2 and the CRA.

2.1.1 Subcontracting

The Supplier shall ensure that any subcontractors comply with the same (cyber) security obligations as the Supplier under this Agreement. The Supplier shall at all times remain responsible for compliance with these obligations by its subcontractors.

2.1.2 (Cyber) liability

The Supplier shall be liable for all direct and indirect damage and loss resulting from a breach of the security obligations under this Agreement. This liability shall not be limited by any other clause in this Agreement.

2.1.3 Contract termination

Upon termination of this Agreement, the Supplier shall return all IT hardware, software, etc. owned by VDL Groep and transfer all data/activities in a format compatible with open standards.

2.1.4 Location

The Supplier shall perform the services and process the data at the location(s) as specified in this Agreement.

2.1.5 Information security

The Supplier shall implement and maintain appropriate security measures, including security testing, anomaly monitoring, vulnerability management, and security updates/patching.

2.1.6 Right of retention

Unless otherwise agreed, ownership of all materials and data used or created by the Supplier under this Agreement shall pass to VDL Groep upon completion of the services or upon termination of this Agreement.

2.1.7 Right to audit

VDL Groep has the right to conduct audits to check the Supplier’s compliance with the security obligations. The Supplier shall cooperate fully with such audits.

2.2 QUALITY OF THE SUPPLIER

2.2.1 Certifications

The Supplier shall demonstrate that it holds relevant certifications (ISAE, SOC2 Type 2, ISO27001, TISAX, CYRA)

2.2.2 Processes and procedures

The Supplier shall implement appropriate procedures for the following topics:

- security incident management,
- backup management,
- vulnerability management,
- patch management,
- monitoring,
- personnel access,
- background checks (certificates of conduct).

2.2.3 Security updates/patching

The Supplier shall ensure that all systems and applications are regularly updated with the latest security patches to address known security vulnerabilities.

2.2.4 Security incidents

The Supplier shall immediately report any and all security incidents to VDL Groep and shall take all reasonable measures to mitigate the consequences of such incidents.

2.2.5 Security assessments

The Supplier shall regularly conduct security assessments and share the results of these assessments with VDL Groep.

2.2.6 Security standards

The Supplier shall comply with all applicable security standards and guidelines, including but not limited to ISO 27001, NIST 800 series, and the General Data Protection Regulation (GDPR).

2.2.7 Access control

The Supplier shall implement appropriate access control measures to prevent unauthorised access to VDL Groep's systems and data.

2.2.8 Data protection

The Supplier shall protect all personal data processed under this Agreement in accordance with applicable data protection legislation.

2.2.9 Security training

The Supplier shall ensure that all its employees who have access to VDL Groep's systems and data receive appropriate security training.

2.3 QUALITY / AVAILABILITY OF SOFTWARE / SERVICE

2.3.1 Availability

The Supplier shall ensure availability by taking measures with respect to the following issues:

- systems availability (RTO/RPO),
- continuity (escrow, continuity arrangement),
- IT continuity and DR procedures (recovery time),
- supplier performance - monitoring/ SLR/ KPI.

2.3.2 Security testing

The Supplier shall regularly conduct security tests, including vulnerability scans and pen tests, to ensure the security of the systems and data. The Supplier shall report any findings from these tests to VDL Groep.

2.3.3 Vulnerability management

The Supplier shall implement and maintain a vulnerability management programme to identify and remediate known security vulnerabilities in the systems and applications.

WANT TO KNOW MORE?

Feel free to contact us via the details below or click on **vdlgroep.com**

VDL Groep B.V.
Hoevenweg 1
5652 AW Eindhoven
The Netherlands
☎ +31 (0)40 292 50 00
✉ info@vdlgroep.com

12-2024