DANOBATGROUP

Standards for the Use of Danobatgroup Information Systems by Suppliers

Version history

Date	Version	Drawn up by	Record of changes
09 February 2026	1.0	Javier Bermejo	First Version

Information about the document

Name	Standards for the Use of Danobatgroup Information Systems by Suppliers
Version	1.0
Created by	Javier Bermejo
Approved by	

DANOBATGROUP

STANDARDS FOR THE USE OF INFORMATION SYSTEMS FOR SUPPLIERS OF THE DANOBATGROUP

1. PURPOSE AND SCOPE

1.1. The purpose of this document is to establish the general conditions governing access to, use, safeguarding and security of DANOBATGROUP's information systems, networks, digital platforms and equipment by suppliers who, within the framework of a contractual or commercial relationship, require access to such systems or process information of the Group.

1.2. These rules apply to all DANOBATGROUP companies (hereinafter, "DANOBATGROUP") and are binding on any supplier, subcontractor or authorised third party (hereinafter, the "SUPPLIER") that directly or indirectly accesses, stores, processes or manages information, data, software or technological infrastructure owned by DANOBATGROUP.

1.3. These rules apply regardless of the channel or means of access used, including, but not limited to, the Supplier Extranet, the e-procurement platform (SRM), VPN connections, ERP systems, corporate email, internal applications, collaboration tools or future digital platforms that may be implemented.

1.4. Acceptance of this document is an essential condition for the granting or maintenance of access rights to DANOBATGROUP's information systems. Failure to comply with these Standards may result in the immediate suspension of access and the application of contractual or legal measures.

2. IDENTIFICATION OF THE PARTIES

- DANOBATGROUP, S. COOP., with registered office at Arriaga Kalea, 20, Elgoibar, Guipúzcoa, Spain, owner of the information systems and responsible for their management.
- The SUPPLIER, being a legal entity or natural person that maintains commercial or contractual relations with any DANOBATGROUP company and that accesses such systems either directly or through its personnel or subcontractors.

3. GENERAL PRINCIPLES AND OBLIGATIONS OF THE SUPPLIER

3.1. The SUPPLIER undertakes at all times to comply with the "Danobatgroup Information Security Policy" and with all applicable legislation, including Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR), Organic Law 3/2018, Law 11/2022 on Telecommunications, and the standards derived from ISO/IEC 27001 and ISO/IEC 27002.

3.2. The SUPPLIER shall be responsible for ensuring that its personnel, subcontractors or agents also comply with the obligations set out in this document.

3.3. Access to systems shall be granted on the principle of least privilege, so that only those permissions strictly necessary for the performance of assigned tasks shall be granted.

3.4. The SUPPLIER shall use the information systems in good faith, with due diligence and for legitimate purposes only, and shall refrain from any improper, unlawful or unauthorised use or any use contrary to DANOBATGROUP's interests.

4. CREDENTIALS AND ACCESS CONTROL

4.1. Access credentials (username, password or digital certificate) are personal and non-transferable. The SUPPLIER shall be fully responsible for their custody and use.

4.2. Sharing credentials, using another user's credentials or using them to access unauthorised information or systems is expressly prohibited.

4.3. The SUPPLIER undertakes to change the password at the intervals indicated by DANOBATGROUP and to immediately notify DANOBATGROUP of any suspected compromise or loss of credentials.

4.4. Any creation, revocation or modification of access rights must be requested and managed through the channels defined by the IT department of DANOBATGROUP.

4.5. DANOBATGROUP may suspend or revoke, at any time and without prior notice, access rights for security reasons, termination of the contractual relationship, non-compliance, or changes in service organisation.

5. USE OF CORPORATE EQUIPMENT AND DEVICES

5.1. The equipment (laptops, desktop computers, mobile phones or tablets) that DANOBATGROUP delivers or makes available to the SUPPLIER shall be used exclusively for professional purposes related to the contracted services.

5.2. The following actions are expressly prohibited:

- Installing unauthorised or unlicensed software.
- Connecting external devices without prior validation (USB devices, external drives, etc.).
- Modifying security settings or attempting to obtain administrator privileges.
- Accessing content or services that may compromise network security (e.g. Dark Web services, torrent platforms, etc.).

5.3. DANOBATGROUP may install **remote management, inventory, encryption, EDR, corporate antivirus or MDM** tools in order to ensure system security, perform updates, isolate compromised equipment and ensure traceability of actions.

5.4. The SUPPLIER shall not have local administrator permissions unless authorised in writing.

5.5. Equipment must be physically secured (locking of the session during absences, secure storage outside working hours, prohibition of sharing).

5.6. In case of loss, theft or damage to the equipment, the SUPPLIER shall immediately notify the IT department by sending an email to **zibersegurtasuna@danobatgroup.com**.

6. REMOTE ACCESS AND EXTERNAL CONNECTIONS

6.1. Remote access shall be carried out exclusively through the corporate VPN or other encrypted mechanisms approved by DANOBATGROUP.

6.2. Devices used to establish remote connections must have up-to-date anti-virus, active firewall, up-to-date security patches and protected network configuration.

6.3. The SUPPLIER shall not connect from public or unsecured networks (e.g. open wifi in airports or cafés) without using a VPN.

6.4. The SUPPLIER may not install or use remote access tools (TeamViewer, AnyDesk, etc.) without express written authorisation.

7. INFORMATION AND DOCUMENTATION MANAGEMENT

7.1. All information and documentation owned by DANOBATGROUP shall be stored on the network drives, servers or official platforms designated for each project.

7.2. Copying, transferring or storing corporate information on personal devices, public cloud services or unauthorised external media is not permitted.

7.3. DANOBATGROUP shall not be liable for the loss or destruction of data stored outside its authorised environments.

7.4. The data and information generated or processed by the SUPPLIER within the framework of its relationship with DANOBATGROUP shall be confidential and shall remain the exclusive property of DANOBATGROUP.

7.5. On termination of the contract or service, the SUPPLIER shall return or delete all information and documentation in its possession, without keeping any copies, unless legally obliged to do so.

8. CONFIDENTIALITY

8.1. “Confidential Information” shall mean any information of a technical, commercial, financial, operational, strategic or any other nature to which the SUPPLIER has access as a result of its relationship with DANOBATGROUP, whether in written, oral or electronic format.

8.2. The SUPPLIER shall:

- Not disclose Confidential Information to third parties without prior written authorisation.
- Use it exclusively for the performance of contractual obligations.
- Take reasonable measures to prevent its loss, alteration or unauthorised access.

8.3. The obligation of confidentiality shall extend to all personnel, subcontractors and third parties involved in the provision of the services.

8.4. The obligation of confidentiality shall remain in force for the duration of the contractual relationship and for a minimum period of five (5) years following its termination.

9. PROTECTION OF PERSONAL DATA

9.1. If the SUPPLIER accesses personal data for which DANOBATGROUP is the data controller, it shall act as Data Processor and shall enter into the corresponding data processing agreement in accordance with Article 28 of the General Data Protection Regulation (GDPR).

9.2. The SUPPLIER shall process personal data solely in accordance with the documented instructions of DANOBATGROUP and shall not use such data for its own purposes or disclose them to third parties.

9.3. The SUPPLIER shall implement appropriate technical and organisational measures to ensure the confidentiality, integrity, availability and resilience of the personal data processed.

9.4. In the event of a personal data breach, the SUPPLIER shall notify DANOBATGROUP without undue delay and, in any event, within 24 hours of becoming aware of the breach.

9.5. Upon termination of the contractual relationship, the SUPPLIER shall return or securely delete all personal data and any copies thereof and shall provide documentary evidence of such deletion.

10. MANAGEMENT OF SECURITY INCIDENTS

10.1. The SUPPLIER shall implement internal procedures for the detection, notification and management of security incidents affecting DANOBATGROUP's systems or information.

10.2. Any security incident shall be reported immediately and without undue delay to zibersegurtasuna@danobatgroup.com, including the following information:

- Date and time of detection.
- Nature of the incident.
- Systems or information affected.
- Containment and mitigation measures implemented.

10.3. The SUPPLIER shall execute all necessary corrective and containment actions to prevent the spread or impact of the incident and shall submit a comprehensive incident resolution report within a maximum period of 72 hours.

10.4. DANOBATGROUP may require additional evidence, documentation or audits arising from the incident.

11. AUDITS AND COMPLIANCE CHECKS

11.1. DANOBATGROUP may, directly or through designated third parties, carry out periodic or ad hoc audits on the security procedures of the SUPPLIER to verify compliance with this document.

11.2. The SUPPLIER undertakes to cooperate fully, facilitating access to the necessary information, documentation and evidence.

11.3. DANOBATGROUP may require the correction of detected deficiencies, and the SUPPLIER must implement the corrective actions within the deadlines indicated.

12. LIABILITY AND SANCTIONS

12.1. The SUPPLIER shall be liable for any direct or indirect loss or damage suffered by DANOBATGROUP as a result of a breach of these standards, including financial losses, administrative penalties or reputational harm.

12.2. Failure to comply with these standards may result in the immediate suspension of access, termination of the contract and/or claims for damages.

12.3. DANOBATGROUP shall not be liable for damages caused by improper use of the systems or negligent actions of the SUPPLIER.

13. DURATION AND VALIDITY

13.1. These standards shall be applicable from the date of acceptance by the SUPPLIER and shall remain in force throughout the contractual relationship and for as long as the SUPPLIER maintains active access to DANOBATGROUP systems.

13.2. DANOBATGROUP may modify these standards at any time by notifying the affected suppliers or by publishing them on the official platforms. Continued use of the systems shall constitute acceptance.

14. APPLICABLE LAW AND JURISDICTION

This document shall be governed by and construed in accordance with Spanish law. For the resolution of any dispute arising out of or in connection with this document, the parties expressly submit to the Courts and Tribunals of Eibar, expressly waiving any other jurisdiction to which they may otherwise be entitled.

15. ACCEPTANCE

The SUPPLIER declares that it has read, understood and fully accepted these Standards for the Use of DANOBATGROUP Information Systems and undertakes to comply with them and to ensure compliance by its personnel, agents and subcontractors.

Date and Signature of the supplier