IRRICONTROL ONE PLATFORM INFORMATION SECURITY POLICY

Information Security and Cyber Defense

1. PURPOSE AND SCOPE

The **IRRICONTROL ONE Platform**, operated by **IRRICONTROL CONTROLE INTELIGENTE DE IRRIGAÇÃO S.A.** ("**IRRICONTROL**"), is a technologically mission-critical solution for the automation and telemetry of agricultural systems on a global scale. This Information Security Policy (ISP) sets out the specific technical and operational requirements for data protection on the IRRICONTROL ONE Platform, a global SaaS automation and telemetry service.

1.1. Scope of Application

This ISP applies in full to:

- Cloud infrastructure (AWS, Azure, Google Cloud)
- The Platform's web and mobile applications
- Connected IoT devices (Nexus, SmartConnect, Irripump)
- Customer data across 26 jurisdictions

Reference: For general corporate guidelines on security, awareness, training and sanctions, refer to the Corporate Information Security Policy of Grupo Bauer do Brasil.

2. GENERAL GUIDELINES AND ALIGNMENT WITH TECHNICAL STANDARDS

This ISP is structured on global information security best practices and is directly aligned with the guidelines set out in the international technical standards **ABNT NBR ISO/IEC 27001** (Information Security Management System – ISMS) and **ABNT NBR ISO/IEC 27002** (Information Security Controls), as well as with the cybersecurity and data protection laws in force in each jurisdiction of operation.

3. MANDATORY REQUIREMENTS FOR THE PROCUREMENT AND ACQUISITION OF SYSTEMS (IT/IS)

In line with the corporate governance best practices of its economic group, any acquisition, lease, in-house development or procurement of systems, software, computing solutions and applications (whether internal or third-party) that will integrate with or support the Irricontrol One Platform must mandatorily comply with the following security requirements:

3.1. Managed Administrator User

Any system procured or developed must provide for the mandatory definition of an administrator user with full and unrestricted access. This administrator access must be managed and controlled exclusively by the internal IT/IS team of **IRRICONTROL**; exclusive access by third parties or vendors is prohibited.

3.2. Prior Approval and Testing

No computing solution or software may be acquired, leased or negotiated without the prior, formal and written approval of the IT/IS technical team of **IRRICONTROL**. The technical team will perform vulnerability testing, network architecture analysis and verification of compliance with the LGPD, the GDPR and other applicable laws before issuing a favorable opinion.

3.3. Mandatory Proof of Concept (PoC) or Proof of Value (PoV)

Before closing any contract for the acquisition or lease of new third-party systems or tools, a Proof of Concept (PoC) or Proof of Value (PoV) must be carried out at no cost to **IRRICONTROL**. This stage must actively involve the IT/IS technical teams and the company's requesting area, with the aim of validating:

- The technical feasibility of integration with the Irricontrol One Platform;
- Compliance with security and data encryption requirements;
- The stability and performance of the solution in an approved test environment.
- Compliance with data localization requirements in jurisdictions that require them.

---

4. TECHNICAL AND OPERATIONAL SECURITY CONTROLS

IRRICONTROL adopts rigorous technical controls to mitigate the risk of security incidents and data leaks on the Platform.

4.1. Logical Access Control

- **Multi-Factor Authentication (MFA)**: Mandatory for all system administrators, developers and employees with access to the Platform's server infrastructure;
- **Privilege Management**: Strict application of the principle of least privilege (*Need-to-Know*). Employees have access only to the information necessary to perform their duties;
- **Access Revocation**: Immediate deactivation of access credentials upon the termination of employees or of contracts with service providers.

4.2. Encryption and Data Protection

- **Data in Transit:** All communication between field devices (IoT), Users' applications and the Platform's servers is protected by encryption using high-standard security protocols (HTTPS, SSL/TLS);
- **Data at Rest:** Personal data, access credentials and critical operational information stored in cloud databases are protected by strong encryption (AES-256).

4.3. Monitoring, Logs and Auditing

- **Log Generation:** The Platform records detailed logs of all critical activities, including login attempts, privilege changes, commands sent to irrigation pivots and database access;
- **Log Centralization and Protection:** Logs are centralized on dedicated audit servers and protected against alteration or deletion (write-only logs);

This document is controlled by the Information Security department. All rights to this document are reserved. Reproduction, use or disclosure to third parties without the express authorization of BAUER is prohibited. Copies of this document will be considered "uncontrolled" unless otherwise indicated and may be deemed intellectual property, and any infringer will be subject to all sanctions and the full weight of the applicable legislation.

- **Vulnerability Analysis:** Periodic security scans and penetration tests (pentests) of the Platform's infrastructure to proactively identify and remediate vulnerabilities.

5. CLOUD INFRASTRUCTURE AND BACKUPS

The Irricontrol One Platform infrastructure is hosted with international-standard cloud providers (such as AWS, Azure or Google Cloud), which offer high resilience and compliance with global security standards (such as SOC 2 and ISO 27001).

5.1. Backup and Disaster Recovery Policy

- **Frequency**: Periodic, automated backups of all of the Platform's operation and registration databases;
- **Secure Storage**: Backups are encrypted and stored in separate geographic zones (geographic redundancy) to ensure business continuity in the event of natural disasters or critical infrastructure failures;
- **Restoration Testing**: Semiannual backup restoration tests to ensure the effectiveness and speed of the disaster recovery plan (DRP).

6. SECURITY INCIDENT MANAGEMENT AND DATA BREACH RESPONSE

In compliance with the LGPD and the ISO 27035 standards, **IRRICONTROL** maintains a structured cybersecurity incident response plan.

6.1. Incident Response Workflow

1. **Identification and Containment**: Upon any suspected or confirmed incident (such as an intrusion, data leak or critical unavailability), the IT/IS technical team will immediately isolate the affected systems to contain the threat;
2. **Analysis and Diagnosis**: Detailed digital forensic investigation to identify the source of the failure, the extent of the affected data and the necessary remediation measures;
3. **Incident Notification**:
    - **Urgent Communication to the Customer: IRRICONTROL** will notify the Customer urgently and immediately of any incident or suspected incident involving personal data under its responsibility;
    - **Communication to Authorities:** If the incident poses a material risk or harm to data subjects, IRRICONTROL will assist the Controller (Customer) in notifying Brazil's National Data Protection Authority (ANPD), the equivalent data protection authorities in other countries (such as the CNIL in France or the ICO in the United Kingdom) and the affected data subjects within the applicable legal deadline (72 hours under the GDPR, 15 business days in Brazil, as applicable).

7. AWARENESS AND TRAINING

This document is controlled by the Information Security department. All rights to this document are reserved. Reproduction, use or disclosure to third parties without the express authorization of BAUER is prohibited. Copies of this document will be considered "uncontrolled" unless otherwise indicated and may be deemed intellectual property, and any infringer will be subject to all sanctions and the full weight of the applicable legislation.

Information security depends on human behavior. **IRRICONTROL** conducts mandatory semi-annual awareness training on information security, privacy and the LGPD for all of its employees and service providers.

8. SANCTIONS AND PENALTIES

Non-compliance with the guidelines and rules set out in this ISP by employees or service providers of **IRRICONTROL** will constitute serious misconduct, subjecting the offender to the appropriate disciplinary measures (warning, suspension, dismissal for cause), in addition to the civil and criminal sanctions applicable under Brazilian law and the laws of the jurisdictions where the Platform operates.

This document is controlled by the Information Security department. All rights to this document are reserved. Reproduction, use or disclosure to third parties without the express authorization of BAUER is prohibited. Copies of this document will be considered "uncontrolled" unless otherwise indicated and may be deemed intellectual property, and any infringer will be subject to all sanctions and the full weight of the applicable legislation.