INFORMATIONSSICHERHEITSRICHTLINIE DER PLATTFORM IRRICONTROL ONE

Informationssicherheit und Cyberabwehr

1. ZWECK UND GELTUNGSBEREICH

Die **Plattform IRRICONTROL ONE**, betrieben von der **IRRICONTROL CONTROLE INTELIGENTE DE IRRIGAÇÃO S.A.** („**IRRICONTROL**"), ist eine technologisch hochkritische Lösung für die Automatisierung und Telemetrie landwirtschaftlicher Systeme im weltweiten Maßstab. Diese Informationssicherheitsrichtlinie (ISR) legt die spezifischen technischen und betrieblichen Anforderungen an den Datenschutz auf der Plattform IRRICONTROL ONE fest, einem weltweiten SaaS-Dienst für Automatisierung und Telemetrie.

1.1. Geltungsbereich

Diese ISR gilt uneingeschränkt für:

- Cloud-Infrastruktur (AWS, Azure, Google Cloud)
- Web- und Mobilanwendungen der Plattform
- Vernetzte IoT-Geräte (Nexus, SmartConnect, Irripump)
- Kundendaten in 26 Rechtsordnungen

Verweis: Allgemeine konzernweite Vorgaben zu Sicherheit, Sensibilisierung, Schulung und Sanktionen finden Sie in der konzernweiten Informationssicherheitsrichtlinie der Grupo Bauer do Brasil.

2. ALLGEMEINE GRUNDSÄTZE UND AUSRICHTUNG AN TECHNISCHEN NORMEN

Diese ISR beruht auf weltweit anerkannten Best Practices der Informationssicherheit und orientiert sich unmittelbar an den Vorgaben der internationalen technischen Normen **ABNT NBR ISO/IEC 27001** (Informationssicherheits-Managementsystem – ISMS) und **ABNT NBR ISO/IEC 27002** (Informationssicherheitsmaßnahmen) sowie an den in der jeweiligen Rechtsordnung geltenden Gesetzen zu Cybersicherheit und Datenschutz.

3. VERBINDLICHE ANFORDERUNGEN AN BESCHAFFUNG UND ERWERB VON SYSTEMEN (IT/IS)

Im Einklang mit den Best Practices der Corporate Governance ihrer Unternehmensgruppe muss jeder Erwerb, jede Anmietung, jede Eigenentwicklung und jede Beauftragung von Systemen, Software, IT-Lösungen und Anwendungen (intern oder von Dritten), die in die Plattform Irricontrol One integriert werden oder diese unterstützen, zwingend die folgenden Sicherheitsanforderungen erfüllen:

3.1. Verwalteter Administrator-Benutzer

Jedes beauftragte oder entwickelte System muss zwingend einen Administrator-Benutzer mit vollständigem und uneingeschränktem Zugriff vorsehen. Dieser Administratorzugang ist ausschließlich vom

internen IT/IS-Team von **IRRICONTROL** zu verwalten und zu kontrollieren; ein exklusiver Zugriff durch Dritte oder Lieferanten ist unzulässig.

3.2. Vorherige Genehmigung und Tests

IT-Lösungen oder Software dürfen nur mit vorheriger, förmlicher und schriftlicher Genehmigung des technischen IT/IS-Teams von **IRRICONTROL** erworben, angemietet oder verhandelt werden. Vor Abgabe einer positiven Stellungnahme führt das technische Team Schwachstellentests, eine Analyse der Netzwerkarchitektur und eine Prüfung der Konformität mit der LGPD, der DSGVO und sonstigen anwendbaren Gesetzen durch.

3.3. Verpflichtender Proof of Concept (PoC) oder Proof of Value (PoV)

Vor dem Abschluss eines Vertrags über den Erwerb oder die Anmietung neuer Systeme oder Werkzeuge Dritter ist zwingend ein für **IRRICONTROL** kostenloser Proof of Concept (PoC) oder Proof of Value (PoV) durchzuführen. Daran sind die technischen IT/IS-Teams und der anfordernde Unternehmensbereich aktiv zu beteiligen, um Folgendes zu validieren:

- die technische Machbarkeit der Integration in die Plattform Irricontrol One;
- die Einhaltung der Anforderungen an Sicherheit und Datenverschlüsselung;
- die Stabilität und Leistung der Lösung in einer freigegebenen Testumgebung.
- die Einhaltung der Anforderungen an die Datenlokalisierung in Rechtsordnungen, die diese vorschreiben.

---

4. TECHNISCHE UND BETRIEBLICHE SICHERHEITSMASSNAHMEN

IRRICONTROL setzt strenge technische Maßnahmen ein, um das Risiko von Sicherheitsvorfällen und Datenabflüssen auf der Plattform zu minimieren.

4.1. Logische Zugriffskontrolle

- **Multi-Faktor-Authentifizierung (MFA)**: Verpflichtend für alle Systemadministratoren, Entwickler und Mitarbeiter mit Zugriff auf die Server-Infrastruktur der Plattform;
- **Berechtigungsmanagement**: Strikte Anwendung des Prinzips der minimalen Rechtevergabe (*Need-to-Know*). Mitarbeiter haben nur Zugriff auf die Informationen, die sie zur Erfüllung ihrer Aufgaben benötigen;
- **Entzug von Zugriffsrechten**: Sofortige Deaktivierung der Zugangsdaten beim Ausscheiden von Mitarbeitern oder bei Beendigung von Verträgen mit Dienstleistern.

4.2. Verschlüsselung und Datenschutz

- **Daten bei der Übertragung:** Die gesamte Kommunikation zwischen den Feldgeräten (IoT), den Anwendungen der Nutzer und den Servern der Plattform ist durch Verschlüsselung mittels Sicherheitsprotokollen nach hohem Standard (HTTPS, SSL/TLS) geschützt;

Dieses Dokument wird von der Abteilung Informationssicherheit gelenkt. Alle Rechte an diesem Dokument sind vorbehalten. Die Vervielfältigung, Nutzung oder Weitergabe an Dritte ohne ausdrückliche Genehmigung von BAUER ist untersagt. Kopien dieses Dokuments gelten, sofern nicht anders angegeben, als „nicht gelenkt“ und können als geistiges Eigentum angesehen werden; Zuwiderhandelnde unterliegen sämtlichen Sanktionen nach geltendem Recht.

- **Daten im Ruhezustand:** Personenbezogene Daten, Zugangsdaten und kritische Betriebsinformationen in den Cloud-Datenbanken sind durch starke Verschlüsselung (AES-256) geschützt.

4.3. Überwachung, Protokollierung und Audit

- **Protokollierung:** Die Plattform erstellt detaillierte Protokolle aller kritischen Aktivitäten, einschließlich Anmeldeversuchen, Berechtigungsänderungen, an die Beregnungsanlagen gesendeten Befehlen und Datenbankzugriffen;
- **Zentralisierung und Schutz der Protokolle:** Die Protokolle werden auf eigenen Audit-Servern zentral gespeichert und gegen Veränderung oder Löschung geschützt (Write-only-Protokolle);
- **Schwachstellenanalyse:** Regelmäßige Sicherheitsscans und Penetrationstests (Pentests) der Plattform-Infrastruktur, um Schwachstellen proaktiv zu erkennen und zu beheben.

---

5. CLOUD-INFRASTRUKTUR UND DATENSICHERUNG

Die Infrastruktur der Plattform Irricontrol One wird bei Cloud-Anbietern nach internationalem Standard (wie AWS, Azure oder Google Cloud) gehostet, die eine hohe Ausfallsicherheit und die Einhaltung globaler Sicherheitsnormen (wie SOC 2 und ISO 27001) bieten.

5.1. Richtlinie für Datensicherung und Notfallwiederherstellung

- **Häufigkeit**: Regelmäßige, automatisierte Datensicherungen (Backups) aller Betriebs- und Registrierungsdatenbanken der Plattform;
- **Sichere Speicherung**: Backups werden verschlüsselt und in getrennten geografischen Zonen (geografische Redundanz) gespeichert, um die Geschäftskontinuität bei Naturkatastrophen oder kritischen Infrastrukturausfällen zu gewährleisten;
- **Wiederherstellungstests**: Halbjährliche Tests der Wiederherstellung von Backups, um die Wirksamkeit und Schnelligkeit des Notfallwiederherstellungsplans (DRP) sicherzustellen.

---

6. MANAGEMENT VON SICHERHEITSVORFÄLLEN UND REAKTION AUF DATENABFLÜSSE

Im Einklang mit der LGPD und den Normen der Reihe ISO 27035 unterhält **IRRICONTROL** einen strukturierten Plan zur Reaktion auf Cybersicherheitsvorfälle.

6.1. Ablauf der Vorfallsreaktion

1. **Erkennung und Eindämmung**: Bei jedem Verdacht auf oder bestätigten Vorfall (wie Eindringen, Datenabfluss oder kritischer Ausfall) isoliert das technische IT/IS-Team die betroffenen Systeme unverzüglich, um die Bedrohung einzudämmen;
2. **Analyse und Diagnose**: Detaillierte digitale forensische Untersuchung zur Ermittlung der Fehlerursache, des Umfangs der betroffenen Daten und der erforderlichen Abhilfemaßnahmen;
3. **Meldung von Vorfällen**:

Dieses Dokument wird von der Abteilung Informationssicherheit gelenkt. Alle Rechte an diesem Dokument sind vorbehalten. Die Vervielfältigung, Nutzung oder Weitergabe an Dritte ohne ausdrückliche Genehmigung von BAUER ist untersagt. Kopien dieses Dokuments gelten, sofern nicht anders angegeben, als „nicht gelenkt“ und können als geistiges Eigentum angesehen werden; Zuwiderhandelnde unterliegen sämtlichen Sanktionen nach geltendem Recht.

- **Dringende Benachrichtigung des Kunden: IRRICONTROL** benachrichtigt den Kunden dringend und unverzüglich über jeden Vorfall oder Verdacht auf einen Vorfall, der personenbezogene Daten in seiner Verantwortung betrifft;
- **Meldung an die Behörden:** Stellt der Vorfall ein erhebliches Risiko oder einen erheblichen Schaden für die betroffenen Personen dar, unterstützt IRRICONTROL den Verantwortlichen (Kunden) bei der Meldung an die brasilianische Datenschutzbehörde (ANPD), an die entsprechenden Datenschutzbehörden anderer Länder (wie die CNIL in Frankreich oder das ICO im Vereinigten Königreich) sowie an die betroffenen Personen innerhalb der gesetzlichen Frist (72 Stunden nach DSGVO, 15 Werktage in Brasilien, je nach Anwendbarkeit).

7. SENSIBILISIERUNG UND SCHULUNG

Informationssicherheit hängt vom menschlichen Verhalten ab. **IRRICONTROL** führt für alle Mitarbeiter und Dienstleister halbjährlich verpflichtende Sensibilisierungsschulungen zu Informationssicherheit, Datenschutz und LGPD durch.

8. SANKTIONEN UND STRAFEN

Verstöße von Mitarbeitern oder Dienstleistern von **IRRICONTROL** gegen die in dieser ISR festgelegten Vorgaben und Regeln stellen ein schwerwiegendes Fehlverhalten dar und ziehen die entsprechenden Disziplinarmaßnahmen (Verwarnung, Suspendierung, Entlassung) nach sich, zusätzlich zu den zivil- und strafrechtlichen Sanktionen nach brasilianischem Recht und dem Recht der Länder, in denen die Plattform tätig ist.

Dieses Dokument wird von der Abteilung Informationssicherheit gelenkt. Alle Rechte an diesem Dokument sind vorbehalten. Die Vervielfältigung, Nutzung oder Weitergabe an Dritte ohne ausdrückliche Genehmigung von BAUER ist untersagt. Kopien dieses Dokuments gelten, sofern nicht anders angegeben, als „nicht gelenkt“ und können als geistiges Eigentum angesehen werden; Zuwiderhandelnde unterliegen sämtlichen Sanktionen nach geltendem Recht.