

Business Continuity Statement

Public summary of resilience and continuity arrangements

Company	Connect.IO Ltd
Document owner	CEO
Version	1.0
Approval date	23 October 2026
Review	At least annually and after material incident/change

Our approach

Connect.IO Ltd maintains a documented Business Continuity Plan designed to support continued delivery of critical business activities during operational, technology, supplier or security disruption. Our approach is proportionate to our operating model and is reviewed as the business, technology environment and customer requirements evolve.

Customer-controlled production

IOblend production environments run exclusively within customer-controlled cloud, on-premises or hybrid infrastructure. Connect.IO Ltd does not host or operate customer production IOblend environments and does not centrally retain customer production data.

Continuity principles

- Distributed and remote-working capability reduces reliance on a single physical location.
- Multiple alternative authorised devices are available if a primary endpoint fails.
- Critical systems use multi-factor authentication and encrypted endpoints.
- Critical company documents are automatically backed up and available through both cloud-synchronised and local working copies.
- Source code is backed up in two separate locations, and restoration from backups is tested.
- Customer support can be maintained through email and phone, with continuity prioritised around applicable contractual SLA obligations.
- Critical supplier dependencies are reviewed and material outages are assessed for customer and operational impact.

Operational recovery

Our internal BCP covers customer communications, engineering and source-code access, business information, security incidents, loss of connectivity or endpoints, supplier outages, loss of key personnel availability, and restoration from backup. Recovery priorities are based on customer impact, security risk and applicable SLA obligations rather than on a single fixed recovery target for every internal service.

Cybersecurity and access continuity

- Multi-factor authentication is used on critical email, source-control and cloud systems.
- Company laptops use full-disk encryption and endpoint protection.
- Important credentials and recovery information are shared securely with authorised personnel to avoid unnecessary single-person dependency.
- Cyber-related recovery uses trusted systems and backups, with integrity checks before normal operation resumes.

Governance and review

Overall responsibility for business continuity rests with senior management. The Business Continuity Plan is reviewed at least annually and following a significant incident, material supplier change, major technology change or significant change to the operating model. Testing includes backup restoration and scenario-based continuity exercises.

Detailed operational recovery instructions, credentials, supplier access information and security-sensitive procedures are deliberately excluded from this public statement. The full Business Continuity Plan can be made available to customers or procurement teams where appropriate and subject to suitable confidentiality controls.

Approval

Approved and signed off on behalf of Connect.IO Ltd by:

Val Goldine

CEO, Connect.IO Ltd

23 October 2026