



COMPLIANCE,  
RISK MANAGEMENT  
AND SECURITY

---

## COMPLIANCE, RISK MANAGEMENT AND SECURITY

### Certified with the latest standards

Our middleware solutions connect over 185,000 secure payment terminals that comply with PCI-PED security requirements and PIN cryptography standards.

Linkly does not have access to cardholder details, PINs, or any other sensitive information as defined by the PCI organisation. We rely on the PCI certifications of our banking partners, complying with all requisite standards. This helps ensure that our customers systems are not exposed to sensitive cardholder information.

### App Hub security

The Linkly App Hub is our proprietary platform that helps our clients integrate alternative payment platforms like Alipay, WeChat Pay, gift cards, loyalty cards and other commerce experiences.

The App Hub supports RSA Signatures, Transport Security Layer 1.2 (TLS 1.2). It is highly flexible to allow new API's to be built into the system rapidly and accurately. With each new capability deployed onto the App Hub, a security certification is completed in alignment with payment companies' requirements.

### Business Continuity Plan (BCP)

Linkly's long history of consistently delivering industry-leading transaction processing availability is maintained through our vigilance in system monitoring, investment in leading fault-tolerant technology and a disciplined approach to capacity planning.

The Linkly business continuity plan has been drafted by payments security and continuity experts in consultation with business leaders within Linkly. It is a living document that remains accurate and relevant through a regular review process.

Linkly continuously reviews BCPs for non-transactions processing systems and annually for the core transaction capability. This testing is low risk since all transaction processing systems and links have capacity on each node exceeding envisaged peak transaction throughput.

The business continuity plan covers all facets of the Linkly business including:

- Finance
- Operations
- Infrastructure
- Services including Help Desks
- Security
- General technology

### Capacity planning

Capacity management is critical for avoiding potential service interruptions and threats to business continuity. Linkly conducts regular capacity management reviews throughout the year to make sure we are ready for sustained peak transaction processing, especially during peak sales periods like Christmas. This process ensures that every component of the payment processing infrastructure can handle loads well in excess of the forecast transaction volumes of the system.

### Our certified risk management framework

The Linkly Risk Management Framework (RMF) follows ISO 31000 standards and provides us with a structure to assess and manage business risks.

The executive leadership team has a crucial role in setting the risk tone for the business and ensures that Linkly aligns with our customers' objectives.

One of our CEO's priorities is ensuring our risk culture is one of accountability and empowerment. We strive for optimal risk management outcomes that enhance our reputation and earn the confidence of our customers.

The executive leadership team has developed a methodology to formally document risks. Its purpose is to measure and manage the risk status and outcomes of business decisions, product development, operations and project design and implementation.

To increase our risk management capacities, the following key initiatives are in progress:

- Investing in risk management systems for better identification, reporting and analytics to deepen our understanding of risk
- Strengthening skills and capabilities across the business
- Improving the structure and quality of data to support risk reporting and decision-making

We are also developing new ways of reporting, identifying and solving customers' issues.

Continuing to focus on these priorities will result in the maturity of Linkly's risk management practices, leading to enhanced customer and risk outcomes.

## Our highly secure data centres

Linkly's infrastructure is designed for complete security, superior availability and maximum transactions throughput. Our transactions processing servers are located in two geographically separate data centres which meet Australian government standards.

### Data Centre No.1 – Global Switch, Sydney Campus, Ultimo

Global Switch's Sydney campus is located on the western edge of Sydney's Central Business District – Australia's financial and commercial hub.

The campus houses two data centres in Sydney East and Sydney West, which together span 73,000 sqm of dedicated technical space.

Due to a network-dense telecommunications presence, the location is ideal for any carrier.

The campus is powered by the largest private high-voltage network in New South Wales and reliability of supply is further assured through the adjacent energy grid which supports 33,000 volts.

Global Switch Sydney has acquired an enviable reputation for operational excellence. Its exceptional engineering and strategic location have made the campus home to a number of the world's largest telecommunications, cloud and financial organisations as well as many state and commonwealth government agencies.

### Site security

- Operations Centre manned 24x7x365
- Security guard patrols 24x7x365
- Continuous CCTV surveillance of external and internal areas
- CCTV records kept for 31 days
- Comprehensive intruder detection and alarms to all areas
- Strict access control procedures to ISO 27001
- Access control using proximity card readers and biometric systems

### Certifications

- ISO 9001
- ISO 14001
- ISO 27001
- ISO 50001
- OHSAS 18001

### Data Centre No.2 – Equinix Mascot, Sydney

Equinix International Business Exchange™ (IBX) SY1 is part of the Equinix Sydney Campus – the most interconnected data centre campus in Australia. It is strategically located in Mascot, a suburb 6km south of the CBD.

One of Australia's most network-dense sites, Equinix provides global peering and interconnectivity opportunities that support a thriving cloud and IT ecosystem.

SY1 is housed in a single-storey pre-cast reinforced concrete building utilising granular temperature monitoring and optimised lighting controls for energy efficiency.

Certifications include SOC 1 Type II, PCI-DSS, SOC 2 Type II, ISO 27001.

### Certifications

- SOC 1 Type II
- PCI-DSS
- SOC 2 Type II
- ISO 27001