consoleconnect

NIS2 compliance statement for **Console Connect**

Console Connect is deeply committed to providing secure and reliable network services for our partners and customers. Recognising the increasing importance of network and cybersecurity in protecting essential services and fostering customer trust, we adhere to the principles and guidelines of the NIS2 Directive. Once implemented by the member states, NIS2 represents a significant step forward in strengthening the security posture of organisations across the EU, contributing to a more resilient digital landscape. It is a key element of the EU's updated cybersecurity framework for electronic communications, critical infrastructure, data protection and e-privacy.

Scope of **NIS2 compliance**

Console Connect understands it is an “important” rather than an “essential” entity under NIS2, and we recognise the directive’s significance and strive to align our network and information security practices as an important entity with its obligations. As a provider of digital infrastructure and connectivity solutions, we understand that our services play a vital role in supporting organisations that may fall under the scope of NIS2. Thus, maintaining a high level of network and cybersecurity is paramount to our operations. We also consider that some of our larger enterprise customers, including those in the public administration, may be considered Essential Entities and that our security posture contributes to meeting their regulatory obligations.

Key **NIS2 risk management requirements**

Console Connect acknowledges the following key requirements of the NIS2 Directive as particularly relevant to our operations and our customers, taking account of state of the art standards:

- **Risk management:** We employ a robust risk management framework, aligned with the principles of ISO 31000, continuously assessing and monitoring our security risks. This includes proactive identification and mitigation of vulnerabilities throughout our software lifecycle.
- **Security policies:** Console Connect maintains comprehensive security policies addressing data protection, access control, incident response, and business continuity. These policies reflect our commitment to maintaining the confidentiality, integrity, and availability of our services.
- **Incident reporting:** We have established clear procedures for reporting and managing security incidents, ensuring timely communication and response. Our dedicated security team constantly monitors our systems for signs of compromise and prioritises addressing reported vulnerabilities.
- **Business continuity and disaster recovery:** Console Connect has developed and regularly tests business continuity and disaster recovery plans to maintain service availability in the event of cyberattacks or disruptions. This includes data backups and robust systems for applying critical security updates.
- **Supply chain security:** We recognise the importance of supply chain security and conduct thorough security audits of all software components, including commercial products and open-source projects, before deployment.

Console Connect's **NIS2 implementation**

Console Connect has implemented the following measures to align with NIS2 obligations in proportion to our risk exposure as assessed, our size as well as incident likelihood and impact:

ISO 27001 certification: We are ISO 27001 certified for:

- The development and operation of the Console Connect Web Application and API
- The operation and provision of core network and system services to PCCW Global and its internal customers, and the management and operations of the SD-WAN service

This certification demonstrates our commitment to information security best practices and provides a strong foundation for NIS2 compliance.

Dedicated security team: We maintain a dedicated team of security professionals who continuously monitor our systems, manage security incidents, and ensure compliance with relevant standards.

Security audits and vulnerability management: We conduct regular security audits of our software and infrastructure and have robust processes for vulnerability management and remediation.

Data security: We prioritise data security, encrypting sensitive data in transit and at rest, implementing strong access controls, and maintaining regular backups.

Employee training: All our developers receive security training as part of their onboarding, reinforcing a security-focused culture across the organisation.

Incident response plan: We have a documented incident response plan and conduct regular exercises to ensure our readiness and responsiveness to security events.

For any enquiries regarding Console Connect's security practices and NIS2 alignment, please contact **infosec@consoleconnect.com**.

Please note that this NIS2 Compliance Statement is current as of 06 November 2024 and may be subject to change to reflect evolving regulatory requirements and our ongoing security enhancements.

consoleconnect

How do I **sign up?**

- Take control
- Cut complexity
- Make interconnection effortless

Easy as a click! Try it for free:
Register now

Australia	Level 3 | 200 Mary Street | Brisbane QLD 4000 | Australia
United Kingdom	7/F 63 St. Mary Axe | London EC3A 8AA | UK
France	2/F 16 rue Washington | 75008 Paris | France
Germany	Schillerstr. 31 | 60313 Frankfurt/M. | Germany
Greece	340 Kifisias Avenue/340 Olimpionikon | Neo Psychiko 154 51 | Athens | Greece
United States	475 Springpark Place | Suite 100 | Herndon | VA 20170 | USA
Singapore	6 Temasek Boulevard | #41-04A/05 | Suntec Tower Four | 038986 | Singapore
Hong Kong	20/F, Telecom House | 3 Gloucester Road | Wan Chai | Hong Kong
Japan	11F – 11A-3 | Imperial Hotel Tower | 1-1-1, Uchisaiwaicho, Chiyoda-ku | Tokyo 100-0011 | Japan
South Africa	Building 12 | 1 Woodmead Drive | Woodmead | Johannesburg 2191 | South Africa
UAE, Dubai	Office 401 & 408 | Level 4 | Arjaan Business Tower| Dubai Media City | Dubai

Have other questions we didn't cover?

Join our community of experts.

www.consoleconnect.com
Talk to us: sales@consoleconnect.com