



Statement of Compliance

Date:3/17/2026

To:Aussie Broadband Limited

Address:3 Electra Avenue, Morwell, VIC 3840, Australia

The statement of Compliance is made in accordance with the Cyber Security (Security Standards for Smart Devices) Rules 2025, made under the Cyber Security Act 2024. The Rules set forth security requirements applicable to the design, manufacture, and operation of certain connected smart devices.

Yealink's products, however, are specifically designed for commercial use. Their positioning, design, sales, and support services are all targeted at enterprise customers and office application scenarios. This positioning has been clearly communicated through multiple channels, including the Company's official website and product documentation. Accordingly, the provisions of the Rules that are intended for "consumer-grade" products are, in principle, not directly applicable to the current market positioning of Yealink's products.

Notwithstanding the foregoing, as a responsible enterprise, Yealink places strong emphasis on user-centric design and continuously monitors the development of relevant laws, regulations, and industry standards, with a view to meeting the evolving needs of enterprise users in diverse working environments. Therefore, with respect to the relevant requirements under the Rules, Yealink hereby makes the following statements:

This Statement applies solely to the Yealink brand products listed in the table below and includes the following:

Product Name	Description
EXP50/EXP55	Color-screen Expansion Module
MP56 E2 Teams/ MP58-WH E2 Teams	Smart Business Phone
SIP-T53W/ SIP-T54W/ SIP-T57W	Prime Business Phone
SIP-T58W Pro	Smart Business Phone
SIP-T85W/SIP-T87W	Ultra Prime Business Phone
SIP-T88W	Ultra Smart Business Phone
W56H/W57R/W59R	IP DECT Phone
W70B	DECT IP Base Station
W90B	DECT IP Multi-Cell Base Station
W90DM	DECT IP Multi-Cell DECT Manager
W73P/W76P/W77P/W79P	DECT IP Phone

1. Password Security: For any device hardware used in its factory condition, a password must be forcibly changed in order to use it normally, and the password is a unique password defined



YEALINK NETWORK TECHNOLOGY CO., LTD

by the user for each product.

2. Vulnerability Disclosure: For Yealink customers and partners, they can report security issues and provide all relevant information through the technical support ticket system (<https://ticket.yealink.com/>). Non-Yealink customers or partners can send an email to security@yealink.com for security researchers. Yealink promises to respond to the report as soon as possible and keep reporter informed of our progress throughout our investigation and/or mitigation of the security issue you reported. For details, please refer to: <https://www.yealink.com/en/trust-center/security-advisories>

3. Security Updates Support: Yealink will provide security updates for our products during the support period. The support period will end on Within 5 years of the product EOS.

1) For the first year after the End-of-Sale (EOS) date, Yealink will offer product support including HW/SW Technical Support, Apply Existing SW Bug Fixes, New Non-Critical SW Bug Fixes, New Critical SW Bug Fixes and New Security Fixes.

2) During the second to fifth year after the End-of-Sale (EOS) date, Yealink will attempt to provide SW bug fixes. During this period, a SW upgrade of the product to a newer existing release will also be seen as a fix to the SW bug. Providing a fix may not be possible in some cases due to the limitation of hardware or software architecture, and Yealink in its sole discretion will determine what fixes, if any, will be provided.

3) Yealink will not offer any New Features/Enhancements support after End-of-Life (EOL). For details, please refer to: <https://www.yealink.com/en/onepage/end-of-life-policy>

We will notify your company of any changes to the above.

YEALINK NETWORK TECHNOLOGY CO.,LTD.

3/17/2026

签署人:

8B480A51066F48E...

Global Technical Manager

yealink

2026/3/19