Security & Support Policy

Author:	Patryk Charydczak
Release date:	28 July 2026
Version:	1.0
Classification:	OPEN

1 Purpose

ADB is committed to maintaining the highest cybersecurity standards on its products throughout their supported lifecycle. This policy provides information on ADB's product security practices, including how to report security vulnerabilities, product security support periods, and other security-related information made publicly available.

This policy supports compliance with all applicable cybersecurity legislations in the jurisdictions where ADB products are supplied, including, where applicable, the Security Standards for Smart Devices under the 2025 Australia Cyber Security Rules, the European Union Cyber Resilience Act (EU) 2024/2847, and other relevant regulatory requirements.

2 ADB Authorized Security Representative

ADB has appointed an Authorized Security Representative ("ASR') to handle security issues on all relevant ADB products.

In particular, ADB ASR is responsible for receiving vulnerability reports, coordinating investigation and remediation, providing status updates, and issuing related reports.

Role	Authorized Security Representative
Organization	ADB
Name / Team	ADB Security Officer Patryk Charydczak
Email	security@adbglobal.com
Telephone	+48 68 4515 151
Postal address	ADB Polska Sp. z o.o. ul. Henryka Sienkiewicza 9 65-443 Zielona Góra Poland
Hours / time zone	0900 – 1600 CET

3 Information Security Framework

ADB has built and maintains an information security and product security framework designed to protect its products, systems and information assets, and to ensure full compliance with applicable statutory, regulatory, and contractual requirements. The framework is based on a risk management approach and is continuously improved to address evolving cybersecurity risks and business requirements.

4 Vulnerability Disclosure

In accordance with all applicable security requirements, we operate a coordinated vulnerability disclosure process. If you discover a security flaw or vulnerability affecting any ADB product, software or supporting service, please proceed as follows:

1. **Report the issue** immediately to ADB Authorized Security Representative via security@adbglobal.com. Please include the specific product model name, software version or service reference, a detailed description of the issue at stake, steps to reproduce, any proof-of-concept, and your contact details. Do not exploit, modify, or exfiltrate data.
2. **Acknowledgement**: ADB will acknowledge receipt of the report within two (2) business days.
3. **Status updates**: ADB will provide status updates to the issue reported at least every 30 days until the issue is resolved or a mitigation plan is agreed.
4. **Resolution**: ADB will develop and distribute a fix (e.g., a firmware/software update) and/or provide mitigations or workarounds.
5. **Coordinated disclosure**: ADB supports coordinated vulnerability disclosure and will work with issue reporters on an appropriate public disclosure timeline.
6. **Regulatory reporting**: Where a reported vulnerability results in, or is associated with, a cybersecurity incident subject to mandatory notification requirements, ADB will fulfil its reporting obligations to the relevant authorities in accordance with applicable law.
7. **Data Breach Notification**: Where a cybersecurity incident involves personal data, ADB will assess its obligations under applicable data protection legislation and notify the relevant supervisory authorities and affected parties where mandated by applicable law.

Scope: This security vulnerability reporting process covers all hardware, firmware, mobile/desktop applications, and supporting web services that ADB provides as part of its products, software and services.

Good-faith testing: If you act in good faith to identify and report a security vulnerability and avoid privacy violations, data destruction, and service disruptions, ADB will not pursue any legal action related to your report. Please allow reasonable time for investigation and remediation before public disclosure.

---

5 Security Updates & End-of-Service (EoS)

ADB provides security updates for relevant products during the Support Period stated below. Security updates include security patches and other updates that address security vulnerabilities affecting ADB product hardware and software.

ADB publishes the Support Period and an end date for each applicable product model and/or major software release. Once published, the Support Period ends at the indicated End of Service date ("EoS") for a given model will not be shortened but it can be extended by ADB.

- **Support Period definition:** The period during which ADB intends to provide security updates for a given product or software release, ending on the published EoS date.

- **End-of-Service (EoS):** After the EoS date, ADB may stop providing security updates for that product/release. Products may continue to function, but they may become exposed to newly discovered vulnerabilities.
- **Customer notification:** ADB will provide notice of upcoming EoS on this page and, where feasible, through product documentation or in-product notifications.
- **Recommended actions at EoS:** Customers should upgrade to a supported version/model, apply all available updates, and follow ADB hardening guidance.
- **Critical issues:** In exceptional cases, ADB may provide guidance or mitigations for high-severity issues after EoS; however, this is not guaranteed.
- **Data & service continuity:** If ADB product or software relies on cloud services, ADB will provide guidance on any service changes tied to EoS and how to retain/export customer data where applicable.

The Support Period for each product is determined individually, taking account the expected product lifetime, contractual commitments, relevant warranties, technology lifecycle and all applicable legal, statutory and regulatory requirements.

If an End of Service date (Support Period) for a given product is defined in a customer agreement, it will take precedence over the published support periods.

Published Support Periods (Security Updates)

ADB Device (Model / Variant)	First Manufacture Date	Last Manufacture Date	Security Updates EoS Date
ADB-2685STWF (Quantum-III) SBB	2025-02-19	2026-08-31 (est)	2027-08-31

6 Disclaimer

ADB will take all necessary precautions and apply its best efforts in the performance of security-related support. However, ADB will take no responsibility for errors, omissions or damages resulting from the use of the information it provides. The support provided by ADB is not designed or intended to address all matters of quality, safety, performance or condition of any product, material, services, systems or processes. ADB and all its affiliates expressly exclude all warranties, conditions and other terms implied by statute or by law (including but not limited to any implied warranties of merchantability and fitness for purpose). All intellectual property rights in any reports, document, graphs, charts, photographs or any other material (in whatever medium) produced by ADB in providing security support shall belong to ADB.

END OF DOCUMENT