BRAVIA Professional Display Security White Paper

Date	Name of Version	Version	Update PiC
Aug.12th 2026	1st Version	0.1	T.Kaneko
Aug.24th 2026	Release version	1.0	T.Kaneko
Aug.31st 2026	Add RDM Version etc	1.1	T.Kaneko
Sep.2nd 2026	Add OTA comment	1.2	T.KANEKO
Sep.2nd 2026	Wording is changed	1.2.1	T.KANEKO

Issue Date

Aug 24th , 2026.

Scope of This White Paper

This white paper focuses on the security system of Sony Pro BRAVIA BZ-P Series Professional Displays (encompassing display hardware, embedded firmware, and on-device features).

Regarding the Content

Product and service specifications may change without notice.

Trademarks

Prohibition of Reproduction, Modification, and Distribution

Table of contents

Introduction

This document outlines the security architecture, hardware trust controls, and software governance implemented for the Sony Pro BRAVIA BZ-P Series Professional Displays (encompassing display hardware, embedded firmware, and on-device features).

Internal Information Security Activities:

Like many companies, Sony faces increasingly sophisticated cybersecurity threats, so the importance of information security continues to grow. In recent years, malicious actors seeking to compromise the information of global companies continue to grow in number, and their attack methods are becoming more advanced. Sony recognizes the importance of cybersecurity, both in achieving financial success for the company and in maintaining the trust of its stakeholders, which include shareholders, customers, employees, suppliers, and business partners. To address this situation and ensure that Sony continues to earn customers' trust, Sony maintains and enhances an information security program.

Risk Management & Strategy:

As part of Sony's risk management framework, Sony maintains and continuously strives to enhance its information security program. This program covers the entire Sony Group and is implemented in accordance with policies and standards, which include cybersecurity risk management and governance frameworks, and guidance, developed by Sony and based on globally recognized industry best practices and standards. The policies define information security responsibilities within Sony and outline certain actions and procedures that officers and employees are required to follow, including with respect to the assessment and management of cybersecurity risks to Sony, including its systems and information. The policies, standards, and guidance are structured to help Sony respond effectively to the dynamically changing environment of cybersecurity threats, cybersecurity risks, technologies, laws, and

regulations. Sony modifies its policies, standards, and guidance as needed to adjust to this changing environment.

If Sony's cybersecurity risk management controls are overcome by a cyber attacker, Sony follows an incident response plan and escalation process as defined in the information security program. The response process includes an assessment of whether an incident may be material, and this assessment is adjusted as necessary as additional facts become known during the incident response. Any incident that is assessed as potentially material is escalated to Sony's senior management and is reported to the two outside Directors in charge of information security on Sony Group Corporation's Board of Directors (the "Board").

Sony has also established policies and processes to help identify and manage cybersecurity risks associated with third parties, including companies that provide services and products to Sony, and companies that hold Sony information or have electronic access to Sony systems or information. The policies and processes include assessment of the cybersecurity and privacy programs at certain third parties, the use of this risk information when making contracting decisions, and the use of contract language that includes cybersecurity and privacy requirements.

Most of the information security program is implemented by Sony employees. Sony also engages the services of external providers to enhance and support its information security program, including leading cyber response specialists as may be needed, and consultants to evaluate and help improve organization, policies, and other aspects of the program.

Structure and Governance of Sony's Information Security Program:

Sony's information security program is under the responsibility of a Senior Executive, specifically, the Sony Group Chief Digital Officer ("CDO"), and the Sony Group Chief Information Security Officer ("CISO"), who reports to the CDO.

Under the leadership of the CDO and CISO, and supported by a global information security team that works across the entire Sony Group, Sony implements the cybersecurity risk management and governance frameworks that are described in its policies and standards. Each business segment of Sony has a senior information security leader, called an Executive Information Security Officer ("EISO"), who reports both to the CISO and to the senior management of the particular business unit. EISOs and their associated teams are responsible for ensuring implementation and operation of the information security program in a way that is tailored to each specific business unit, including as it relates to the assessment and management of cybersecurity risks. The CISO coordinates with the EISOs to monitor the proper implementation and compliance with Sony's cybersecurity policies and standards.

To oversee the information security program, the Sony Group CEO and COO receive regular reports from the CDO, monthly reports from the CISO, additional reports as needed during the response to a cyber incident, and briefings from the CDO and CISO at various times during the year. The head of each Sony business segment also receives the monthly reports from the CDO and the CISO, as well as reports and briefings from the business segment EISO.

Employee Training as a Key Component of Information Security:

Every employee has a critical role to play in protecting Sony's most sensitive information. To increase Sony employees' awareness of information security threats, Sony requires all personnel to receive annual information security

training, where they learn how to report incidents and study the types of behaviors they must avoid in order to reduce risk. Sony employees also regularly receive phishing awareness training, which tests employees' knowledge of how to spot and avoid cyber-attacks delivered through fraudulent emails.

Product Security Activities During Product Development:

With more products connecting to networks, there is a heightened danger of personal information leaks, tampering or destruction of data, product hijacking and other such security issues. As a consequence, it is vital to improve the quality of the security of products and network services.

Sony has a function for collecting security risk-related information from outside experts, researchers and other individuals. Sony assigns managers responsible for the software security of products and has a dedicated department for this purpose. The department coordinates with business units to address issues with the security of products.

Based on the information received, the department assesses the impact of risk on customers from a software security perspective and implements appropriate measures.

Sony also implements security design and response systems in order to deliver products that customers can use with confidence. In 2012, the Sony Security Development Lifecycle was formulated as measures and rules to enhance security quality throughout each phase, from product development and network service planning right up to the time the product is discarded or the network service is terminated. As part of this process, it subjects products and network services to pre-shipping and pre-release inspections, including security risk assessments and the use of product security vulnerability detection tools. These measures and rules are in place for all Sony products and network services, and regular inspections and audits are performed to ensure that they are being adhered to. Sony has also established internal guidelines pertaining to the security of products.

Sony regularly reviews and updates these guidelines, and continues to implement employee training programs to enhance product security. Due to growing concern over security issues relating to the Internet of Things (IoT), regulators in various countries/regions are developing new laws and regulations concerning IoT security. Sony has included requirements for conformance to IoT security regulations in the Sony Security Development Lifecycle. Sony has internal frameworks for collating and ensuring compliance with regulatory requirements in individual countries and regions.

Service Overview

Target Platform:

Sony Professional Display BZ-P Series / Commercial Displays

Notice & Scope:

This document outlines the security architecture, hardware trust anchors, network capabilities, interface management, content protection, and vulnerability governance practices for Sony Pro BRAVIA BZ-P Series displays. It builds upon established platform baselines and incorporates modern European regulatory requirements (e.g., RED Cybersecurity Directive).

Executive Summary & Definitions

Sony Pro BRAVIA displays are designed to meet stringent commercial and enterprise security standards. Operating across corporate, digital signage, education, and retail environments, Pro BRAVIA provides robust isolation between system services, user data, and external interfaces

References

Professional Display BZ-P Manual :

BRAVIA Professional Displays Knowledge Center

Terminology

Term	Definition
Owner	Entities, IT administrators, or business operators who own or manage the BRAVIA Professional Display for operational purposes (e.g., system integrators, facility managers, enterprise IT).
Anonymous End-User	Individual end-users who interact with or view the display without administrative privileges (e.g., meeting participants, hotel guests, visitors).
Pro Settings	Integrated management interface allowing administrators to customize operational behaviors, lock settings UI, and enforce privacy controls.

Hardware & Platform Security

The core foundation of the Pro BRAVIA platform relies on dedicated hardware security primitives implemented directly within the System-on-Chip (SoC) LSI architecture.

Cryptographic Hardware Root of Trust & Secure Boot

● Hardware Root of Trust:

Validation keys are permanently programmed during manufacturing within secure, unreadable memory residing in the dedicated cryptographic processor subsystem of the SoC LSI.

● Secure Boot Flow:

At every power-on sequence, the platform processor computes a cryptographic checksum of the bootloader and system firmware image. This calculated digest is verified against the signed signature stored in Flash memory.

● Tamper Prevention:

If signature mismatch or image corruption is detected, the execution CPU halts system loading immediately, preventing unauthorized firmware execution, ROM flashing, or code injection.

Operating System & Architecture Integrity

Pro BRAVIA models fully comply with AOSP (Android Open Source Project) security policies, enforcing strict boundaries against privilege escalation.

You can refer to https://source.android.com/docs/security.

OS Security Controls

● CTS (Compatibility Test Suite) Compliance:

Every released software build passes Google CTS verification to guarantee platform integrity.

● Locked Bootloader:

Pro BRAVIA enforces stringent bootloader access controls combined with fault-tolerant recovery mechanisms to prevent the execution of unauthorized firmware and custom ROMs.

- Restricted Device Unlock (Console Lock):
  The platform restricts console-level command interfaces, blocking unauthorized device unlock operations and preventing the flashing of custom recovery images or unsigned third-party operating systems.

- Integrity Verification & Automated Rollback:
  System images undergo cryptographic signature verification against the hardware trust anchor during power-on and update sequences. If an unauthorized, corrupted, or tampered image is detected, the execution flow triggers an automated rollback mechanism to restore and boot the previous validated system image, ensuring both security and operational resilience.

You can refer to https://source.android.com/docs/security/features/verifiedboot.

● Privilege Isolation:

Root access is strictly prohibited. System-level privileges are withheld from third-party applications.

● Application Sandboxing:

Applications execute within isolated SELinux sandboxes with restricted IPC (Inter-Process Communication).

Network & Communication Security

Control Protocol Authentication (IP Control/IRCC)

Network-based management interfaces (IP Control/IRCC) utilize robust pre-shared key or token-based authentication mechanisms to block unauthorized command injection over LAN/WLAN.

CA Certificate & Runtime Security

● HTML5 Application Runtime:

Pre-loaded Root CA certificates comply with standard Android TV / AOSP infrastructure, restricting connection establishing strictly to trusted TLS endpoints.

● Wi-Fi Security Policy (RED-DA Compliance):

To satisfy European Radio Equipment Directive (RED-DA) provisions, Wi-Fi access point functionality and network connections require a mandatory minimum 16-character Pre-Shared Key (PSK) password policy.

● Wi-Fi Security Policy (Wi-Fi Enterprise)

To meet stringent enterprise network security requirements, Pro BRAVIA displays support WPA2/WPA3-Enterprise protocols (IEEE 802.1X / EAP authentication framework).

- Custom CA Certificate Deployment: System administrators can securely install and manage custom enterprise Root and Intermediate Certificate Authority (CA) certificates on the display via Pro settings or enterprise MDM/EMM platforms.

- Server Authentication & MitM Prevention: During IEEE 802.1X authentication

(including EAP-TLS and PEAP), the display validates RADIUS and authentication server identities against installed CA certificates, mitigating Man-in-the-Middle (MitM) exploits and preventing unauthorized network association.

Firmware Package Security

Firmware Package (PKG) Security & Integrity Protection
Firmware update packages (PKG) deployed across Pro BRAVIA displays—whether distributed Over-The-Air (OTA) or via USB storage media—are secured end-to-end against unauthorized modification, tampering, and malicious execution.

- Cryptographic Signature & Integrity Verification:
  Every official firmware package is digitally signed in a secure Sony build environment. Prior to executing an update, the display validates the package's digital signature and hash digest against trusted public keys tied to the hardware root of trust within the SoC subsystem, strictly rejecting unsigned, corrupted, or tampered images.

- Secure Transport (OTA Updates):
  Network-based OTA update deliveries are enforced over encrypted TLS channels, mitigating Man-in-the-Middle (MitM) attacks, eavesdropping, and payload alteration during transit.

- Fault-Tolerant Fail-Safe Mechanism:
  The update process incorporates resilient fail-safe measures to preserve system integrity and prevent device bricking in the event of power loss or package corruption during deployment.

Network Configuration Requirement (OTA Service):

In enterprise network environments with restricted egress traffic, firewalls and proxy servers must be configured to permit outbound HTTPS (Port 443) communication to the following Sony endpoints to ensure proper device authentication and delivery of OTA packages:

1. *.auth.dip.sony.tv (Wildcard domain for authentication and token validation services)

2. api.erabu.sony.tv (Endpoint for update queries, provisioning, and payload retrieval)

Interface & Connectivity Management

To eliminate unauthorized physical or wireless attack vectors, administrators can individually disable or restrict hardware interfaces via the System and Pro settings menus:

Interface / Feature	Control & Disabling Method	Security Objective
RS-232C Control	Settings > Remotes & Accessories > RS232C control	Prevents physical serial port unauthorized command execution.
HDMI CEC (BRAVIA Sync)	Settings > Inputs > External inputs > BRAVIA Sync settings	Blocks unauthorized CEC signal injection across connected AV hardware. Compliant with CEC version1.4
Bluetooth	Settings > Remotes & Accessories > Bluetooth settings	Disables wireless pairing with unauthorized peripheral devices.
Built-in Wi-Fi	Settings > Network & Internet > Wi-Fi	Ensures hardwired network isolation when wireless is not required.
AirPlay	Settings > System > Apple AirPlay & HomeKit	Restricts unauthorized wireless screen mirroring in public spaces.

Interface / Feature	Control & Disabling Method	Security Objective
Wi-Fi Access Point	Settings > Pro settings > Wi-Fi access point	Controls display-hosted hotspot capabilities and enforces strong PSK.

Content Protection & Digital Rights Management (DRM)

Pro BRAVIA provides enterprise-grade content protection for broadcast, OTT, and external input streams.

● Streaming DRM Schemes:

- DASH: Google Widevine L1 (cenc scheme), Microsoft PlayReady SL3000

- SmoothStreaming: Microsoft PlayReady SL3000

- HLS: Sample AES

● HDMI Interface Protection:

Compliant with HDCP 2.3 encryption standard across external video inputs.

Operational Security & Pro Settings Controls

Pro settings allow system administrators to transform consumer display interfaces into hardened commercial endpoints.

Data Protection & Privacy Controls

● Automated Data Erasure (Power-Off Trigger):

Upon power cycling or session termination, the system automatically purges stored account credentials in Account Manager and clears cached application storage.

● Anonymous End-User UI Locking:

Hides administrative configuration UI to prevent access to network and security settings.

● Application Control:

Restricts end-users from installing new applications or launching unauthorized pre-installed apps.

● Physical Key & RC Lockout:

Option to disable physical side buttons and IR/Bluetooth remote controller inputs.

● Access Protection:

Modifying Pro settings parameters requires a dedicated key sequence and PIN code authorization.

Vulnerability Management & Governance Lifecycle

Independent Penetration Testing

Sony systematically subjects Pro BRAVIA hardware and firmware architectures to comprehensive security assessments and periodic independent penetration tests conducted by accredited external security auditing firms as well as specialized internal red teams.

Vulnerability Remediation & Patch Management

Identified vulnerabilities are scored according to industry-standard CVSS (Common Vulnerability Scoring System) frameworks. Remediation patches and updated firmware builds are prioritized and released periodically over-the-air (OTA) and via USB service packages.

Internal Security Management Guidelines

Sony enforces rigorous internal security practices governed by defined Security Development Lifecycle (SDL) standards and product security specifications. Upon request and subject to review, high-level summaries of product security frameworks and operational compliance records may be disclosed under a Non-Disclosure Agreement (NDA). Please consult your designated account representative for further details.

Customer Transparency & Information Disclosure

Detailed penetration testing artifacts and technical exploit logs are kept strictly confidential to preserve overall system security across installed bases. However, high-level Executive Summaries outlining audit compliance and remediation status can be provided to corporate clients under a Non-Disclosure Agreement (NDA) to support formal tender and compliance reviews.