

ClickShare security, compliance and certifications snapshot

How Barco manages trust, risk and verification for secure collaboration



Why meeting room security matters

Hybrid collaboration has made meeting spaces more connected and more business critical. It has also increased the number of devices, networks, and third-party services that need to be secured and managed consistently.

Security in meeting rooms needs to support three priorities at the same time:

Protect sensitive information

Meeting rooms routinely handle confidential content, shared data and collaboration activity. Protecting these spaces helps safeguard business information, operations and reputation.

Support secure adoption

Security controls need to fit naturally into daily collaboration. When security is intuitive, users are more likely to work securely without creating workarounds.

Build confidence through verification

Organizations increasingly expect secure-by-design solutions, recognized standards and transparent security processes. Certifications and documented governance help make security easier to evaluate.



Barco's approach to ClickShare security

Trust does not come from one feature or one certification. It comes from a structured approach to how security is governed, built into the product, and maintained throughout the lifecycle.

Governance

Product controls

Lifecycle assurance

Governance



Dedicated security organization: Barco has established a company-wide security structure, with a Security Office driving corporate and product security, supported by auditing as an additional line of defense.



Information Security Management System (ISMS): This formal management framework identifies security risks, defines controls, and drives continuous improvements. It is validated through independent ISO/IEC 27001 certification.



Responsible disclosure plus PSIRT: Barco provides a clear process for reporting vulnerabilities and commits to handling reports confidentially while tracking remediation progress.

What this means

Security is managed through defined responsibilities, recognized frameworks and structured processes.



Security is built into ClickShare through a comprehensive set of product controls that help organizations protect meeting spaces while aligning with their security policies.

Governance

Product
controls

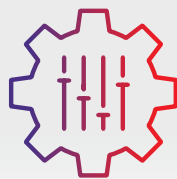
Lifecycle
assurance

Product controls



Security built into the product lifecycle:

ClickShare positions security as a core principle from product design to firmware updates, supported by independent certifications like ISO 27001 and responsible vulnerability disclosure practices.



Configurable security levels:

Administrators can apply predefined security levels to align ClickShare device behavior with organizational policy (e.g., stricter pairing and configuration requirements at higher levels).



Enterprise-ready deployment:

ClickShare is designed for networked meeting rooms and hybrid collaboration, aiming to balance IT-grade protection with an intuitive user experience.

What this means

Organizations can align ClickShare with their security policies while still supporting practical, everyday collaboration.



Long-term security is supported by continuous improvement, combining regular firmware updates, structured vulnerability management, and shared responsibility for secure deployment and operation.

Governance

Product
controls

Lifecycle
assurance

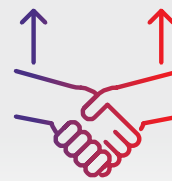
Lifecycle assurance



Ongoing firmware updates: ClickShare includes regular firmware updates as a core part of its security model, with quarterly releases supporting long-term protection across the product lifecycle.



Formal vulnerability disclosure process: Barco provides a structured process for reporting security vulnerabilities through its support portal and PSIRT email, supported by clearly defined responsible disclosure guidelines.



Shared responsibility in deployment: Customers control how solutions are configured and maintained, keeping devices updated and choosing the right security level for their environment.

What this means

Barco provides the processes and update model to support ongoing security, while customers retain configuration control.



What this means for your organization

ClickShare security is designed to support decision-making across IT, security and procurement teams.

Align security with enterprise policy

Certified governance frameworks, configurable controls, and structured vulnerability management support policy-driven deployment.



Balance protection and usability

Security controls are designed to support both adoption and risk reduction, helping users collaborate securely without unnecessary friction.



Scale securely

A consistent security model helps reduce operational complexity across meeting room estates.



Support procurement decisions

Independent certifications, transparent governance, and structured security processes provide objective assurance for supplier evaluation and risk review.



Understanding the security standards and certifications

Certifications should not be seen as decorative logos. They help buyers understand which processes, controls and responsibilities have been independently assessed or aligned with recognized standards.

Certification scope can vary, so organizations should always verify coverage for the specific entity, location or service included in their deployment.

Certifications at a glance

Standard	What it covers	Why it matters to buyers
ISO/IEC 27001:2022	The core framework for an Information Security Management System (ISMS), including risk assessment, security controls, governance, and continual improvement	Provides assurance that security is managed systematically, supported by defined processes, governance, and independent audits.
ISO/IEC 27017:2015	Guidance for implementing information security controls for cloud services, both cloud provider and cloud customer responsibilities).	Helps organizations evaluate cloud security controls and understand shared-responsibility boundaries in hybrid environments.
ISO/IEC 27018:2019	Protection of personal data (PII) in public cloud environments where the provider acts as a PII processor.	Ensures personal data is handled according to recognized privacy practices, supporting privacy due diligence and GDPR obligations.
ISO 9001:2015	Quality Management System (QMS) processes for consistent delivery and continuous improvement.	Provides assurance that products and services are supported by mature processes focused on quality and operational reliability.

Key takeaways

Meeting room technology is now part of enterprise risk. It needs to be evaluated not only for usability, but also for governance, security controls, compliance relevance and lifecycle assurance.

ClickShare supports secure collaboration through:

- Barco's structured security governance and certified Information Security Management System.
- Configurable product controls that help align ClickShare with organizational policy.
- Regular firmware updates and formal vulnerability disclosure processes.
- Recognized certifications that support risk, privacy and procurement reviews.
- A security approach designed to balance protection, usability and scalability.



M00000-R00-0826-PB | Last updated: August 2026

© 2026 Barco nv. All rights reserved. Reproduction in whole or in part without written permission is prohibited. All brand names and product names are trademarks, registered trademarks or tradenames of their respective holders. Due to continued innovation, information and technical specifications are subject to change without prior notice. Please check www.barco.com for the latest specifications.