eventbuilder
enterprise virtual event services

ULTIMATE VIRTUAL EVENTS SECURITY AND COMPLIANCE CHECKLIST

www.eventbuilder.rocks

eventbuilder
enterprise virtual event services

INTRODUCTION

Virtual events are amazing platforms for connection, collaboration, and content delivery, but they come with security and compliance responsibilities that can't be overlooked. As cyber threats become increasingly sophisticated and privacy regulations are tightening, protecting your event data — and your attendee's private information — is a requirement, not simply an option.

We've designed this checklist to help you build a solid security and privacy foundation for your virtual events. Use this guide to evaluate risks, make informed decisions, and make sure your event is secure from the ground up. While no checklist can replace expert guidance and a comprehensive risk management strategy, we're offering you this tool to help you stay organized and proactive throughout your event planning and execution.

eventbuilder
enterprise virtual event services

FOUNDATIONAL PLANNING AND RISK ASSESSMENT

Security starts before your first attendee logs in. A proactive approach to planning and risk assessment can prevent issues before they start. Begin here:

- **Define Event Security** - Classify your event type: public webinar, internal meeting, confidential partner session, earnings call, etc. This sets the tone for your security posture.
- **Identify Potential Threats** - Anticipate the specific risks your event may face based on its sensitivity and audience. Think of threats like unauthorized access, IP theft, phishing, or chat/Q&A abuse.
- **Assess Data Sensitivity** - Document the types of data you'll collect or share—attendee and speaker PII, payment information, chat logs, intellectual property, or other sensitive content.
- Determine Applicable Regulations - Understand which data protection laws apply to your even based on where your organization and your attendees are located. (e.g., GDRP, CCPA/CPRA, HIPAA, industry-specific standards.
- **Assign Security Responsibilities -** Designate team members to key security roles, such as platform setup, content moderation, incident response, and compliance oversight, to ensure nothing falls through the cracks.
- **Allocate a Security Budget** - Confirm that time, budget, and staffing are in place for the tools, training, and expoert support your event may require.

eventbuilder
enterprise virtual event services

PLATFORM SELECTION & VENDOR VETTING

The decisions you make when selecting your platform can either strengthen your defenses or expose you to risk. Choose wisely!

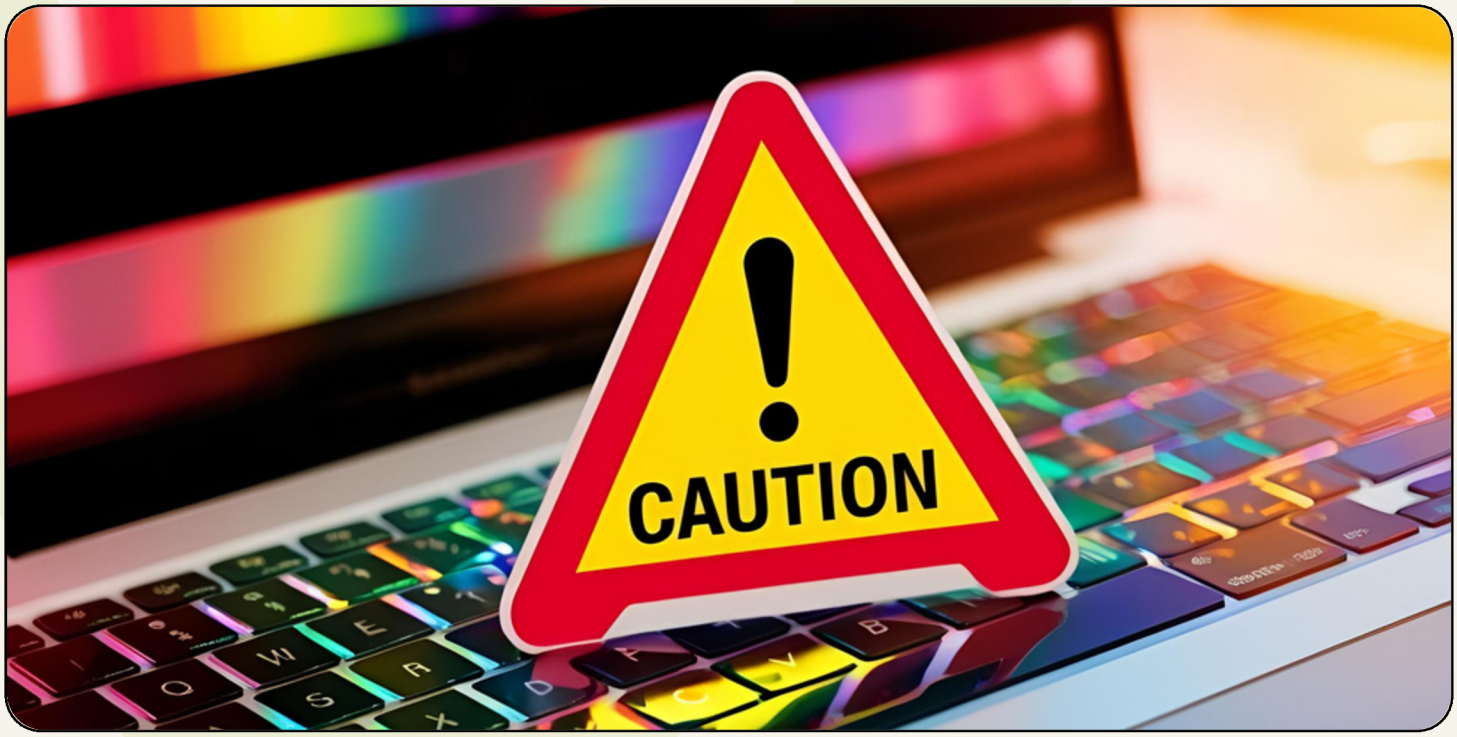
- **Evaluate Core Platform Security** - Compare platforms based on their built-in security capabilities. Look for:
    - **Encryption** - Ensure encryption in transit (TLS) and at rest (AES-256). For high-sensitivity events, explore options for end-to-end encryption (E2EE)
    - **Authentication** - Confirm support for multi-factor authentication (MFA) and single sign-on (SSO) for both internal and external participants.
    - **Access Controls** - Look for features like waiting rooms, role-based permissions, host controls, and passcodes to manage who gets in and what they can do.
    - **Monitoring & Logging** - Check if the platform provides audit logs and real-time monitoring for security oversight and incident tracking.

- **Verify Vendor Compliance** - Request proof of third party certifications such as ISO 27001/27701, SOC 2 Type II, or HIPAA Attestation.
- **Review the Data Processing Agreement (DPA)** - Make sure the vendor offers a clear, comprehensive DPA that aligns with data privacy regulations, such as GDPR and CCPA/CPRA. Don't just accept it—read it!
- **Assess Vendor Support for Security Incidents -** Treat every integration as its own potential risk. From polling tools to CRMs to analytics platforms, each must meet your security and compliance standards. Review their DPAs and ask the tough questions.

eventbuilder
enterprise virtual event services

PLATFORM SELECTION & VENDOR VETTING

- **Vet Third-Party Integrations** - Treat every integration as its own potential risk. From polling tools to CRMs to analytics platforms, each has to meet your security and compliance standards. Review their DPAs and don't shy away from asking tough questions.
- **Leverage Ecosystem Security** - Platforms that operate within secure ecosystems, such as EventBuilder's integration with Microsoft Teams, inherit enterprise-grade identity management, compliance coverage, and data protections. This can simplify vetting and boost overall confidence.



eventbuilder
enterprise virtual event services

SECURE CONFIGURATION & ACCESS CONTROL

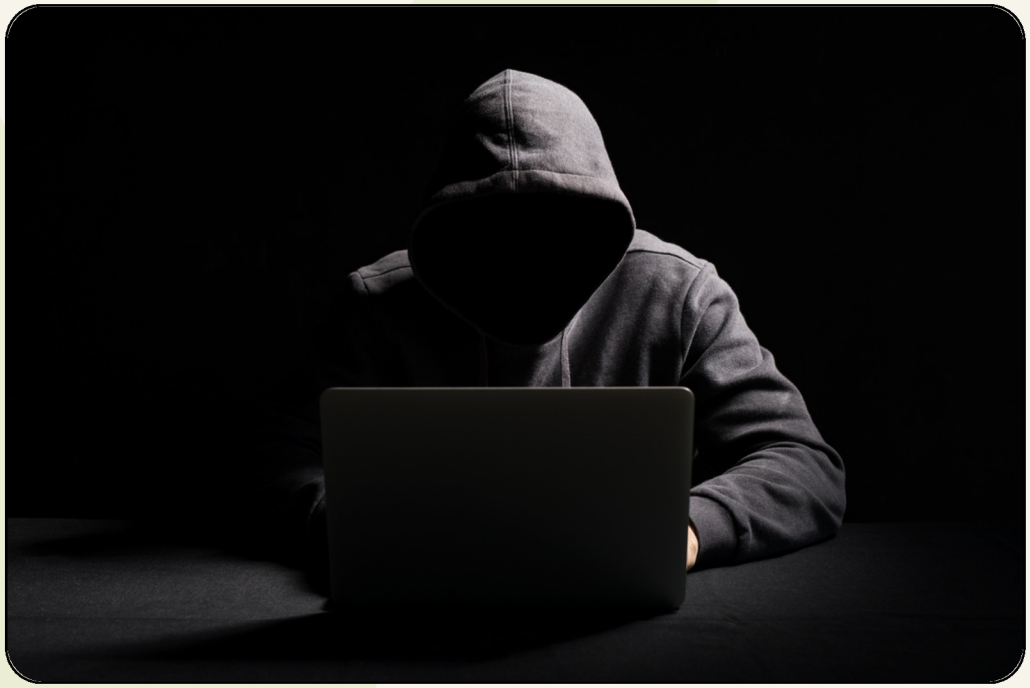
A secure platform is only as secure as its settings. Default configurations are rarely enough—intentional setup is key to minimizing risk and maximizing control. Remember: prevention through precision. It's worth the effort to get it right.

- **Use Unique Meeting IDs** - Skip Personal Meeting IDs for scheduled sessions. By generating a new, unique ID for each event, you reduce the chances of uninvited access.
- **Require Strong Passcodes** - Every event should be protected with a unique, hard-to-hack passcodes. For sensitive events, avoid embedding passcodes in join links.
- **Mandate Registration** - Gate access by requiring attendee registration. This also helps with access control and provides an audit trail if needed.
- **Enable Waiting Rooms** - Add an extra layer of control by holding incoming participants in a lobby / waiting room until they're admitted. This is especially useful for high-touch or confidential sessions.
- **Turn off "Join Before Host" -** Prevent meetings from starting without an authorized host present. It's a small setting with big security implications.
- **Lock Down Screen Sharing** - Set screen sharing permissions to "Host Only" by default. Extend access selectively and intentionally.
- **Disable Unnecessary File Transfer -** Unless it's mission critical, turn off file sharing in chat to lower the risk of malware or unauthorized file distribution.
- **Manage Chat Settings Wisely** - Choose the right chat configuration: public only, moderated, or disable private messages between attendees, depending on your event type.

eventbuilder
enterprise virtual event services

SECURE CONFIGURATION & ACCESS CONTROL

- **Control Muting Behavior** - Every event should be protected with a unique, hard-to-hack passcodes. For sensitive events, avoid embedding passcodes in join links.
- **Require Authentication When Possible -** Gate access by requiring attendee registration. This also helps with access control and provides an audit trail if needed.
- **Lock the Meeting Once it Starts** - Once everyone is in, lock the door behind you. Locking the session helps prevent unwanted late entries or disruptions.
- **Use Advanced Controls When Appropriate** - For high-stakes or regulated events, layer in protections such as multi-factor authentication, IP allowlists, or end-to-end encryption if supported.



eventbuilder
enterprise virtual event services

DATA PRIVACY & COMPLIANCE

Privacy is a cornerstone of your virtual event strategy, so when it comes to attendee data, there's zero room for shortcuts. Respecting privacy rights and complying with global regulations isn't just about checking boxes; it's about earning trust and protecting your brand.

- **Make Your Privacy Policy Easy to Find** - Link to your current, compliant Privacy Policy on all registration forms, event pages, and attendee communication emails. Clarity and transparency are key to staying compliant and signaling to prospects that you take their privacy seriously.
- **Collect Only What You Need** - Stick to data minimization. It's tempting to gather as much attendee data as possible, however, by only requesting the personal information that's essential for the event you build brand trust. Also, be prepared to explain why each data point is necessary.
- **Use Clear GDPR Consent Mechanisms** - Add explicit, opt-in checkboxes—left UNchecked by default—for things like marketing emails, event recordings that capture PII, or sharing attendee info with sponsors. Make opting OUT just as easy as opting IN.
- **Support CCPA/CPRA Requirements** - Include clear options like, "Do Not Sell or Share My Personal Information" and "Limit the Use of My Sensitive Personal Information." These should be visible and accessible right away.
- **Respect Global Privacy Control (GPC) Signals** - Configure your systems to recognize and honor browser-based opt-out signals like GPC. It's a small step with a big privacy impact.

eventbuilder
enterprise virtual event services

DATA PRIVACY & COMPLIANCE

- **Be Transparent About Sponsor Data Sharing** - If you share attendee data with sponsors, disclose it up front. Collect the appropriate consent under GDRP or provide opt-outs under CCPA/CPRA. It's important to have clear, contractual agreements with sponsors about how they can use the data.
- **Define and Document Retention Timelines** - Create a retention policy that outlines how long you'll keep event data: registration lists, recordings, chat logs, etc. and why. Communicate that policy clearly.
- **Have a DSAR Process Ready** - Data Subject Access Requests are rights given to individuals to control their personal data that organizations house. Be prepared to respond to these or consumer rights requests in a timely, transparent, and respectful way. We recommend outlining a clear, internal workflow for verifying and responding to requests within required timeframes.
- **Secure Your Data Storage** - Make sure all your attendee and event-related data is stored securely. Use encryption at rest and enforce strict access controls, especially for recordings and transcripts.

eventbuilder
enterprise virtual event services

SECURE COMMUNICATIONS & CONTENT

The way you share information before, during, and after your event is just as important as the tools you use. Protecting communications and content is a key part of your event's overall security posture.

- **Distribute Links Securely** - Send join links and passcodes directly to registered attendees via confirmation emails or secure platforms. Never post them publicly.
- **Train Presenters on Screen Sharing Best Practices** - Instruct speakers to share specific application windows instead of entire desktops, and to close unrelated apps or browser tabs to avoid accidental exposure.
- **Consider Content Watermarking** - For events involving proprietary or sensitive content, explore visible or forensic watermarking on slides or video to deter leaks and trace unauthorized sharing.
- **Protect Access to Recordings** - Use access controls, expiration settings, and passwords to secure recordings. Disable downloads if the content is sensitive or restricted.
- **Use Secure Channels for Internal Communications** - Keep internal discussions—especially those involving credentials or sensitive planning details—on encrypted, trusted communication platforms.

eventbuilder
enterprise virtual event services

ATTENDEE TRUST AND COMMUNICATION

Security isn't just about infrastructure: it's about communication, clarity, and confidence. Transparency shows your commitment and encourages secure behavior from participants.

- **Share Your Security Commitment Up Front** - Add a short section to your website and registration page that highlights your approach to privacy and security, mentioning features like encryption and platform protections.
- **Link to Core Policies** - Make it easy for attendees to access your Privacy Policy and Code of Conduct. Visible, accessible links promote transparency.
- **Reinforce in Confirmation Emails** - Include key security reminders in your emails: don't share access links, here's where to find our policies, and what to expect.
- **Mention During the Kickoff** - Take a moment during your event's opening remarks to briefly outline the code of conduct, security expectations, and how attendees can reach support if needed.
- **Provide a Clear Support Path** - Be sure your attendees know exactly how to report a technical issue or flag a security concern. A quick response builds trust.
- **Be Open About Data Use** - Clearly explain why you're collecting personal information and how it will be used. If sponsor data sharing is involved, direct attendees to the relevant consent or opt-out options.

eventbuilder
enterprise virtual event services

DURING-EVENT MONITORING AND MODERATION

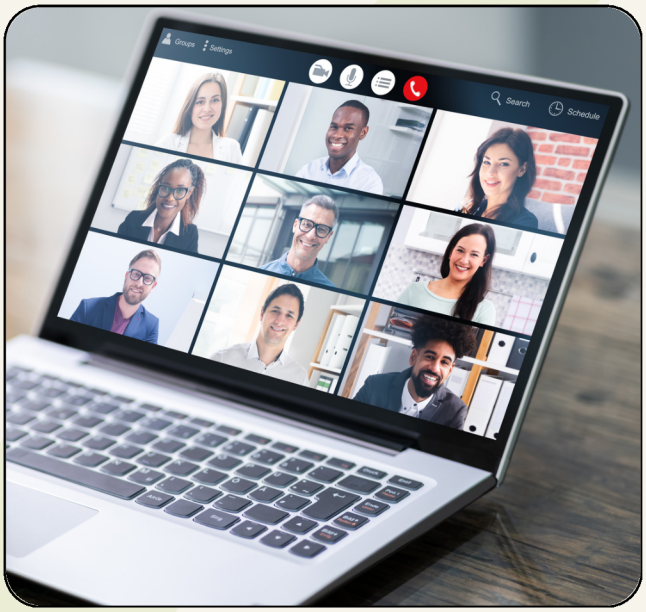
The work doesn't stop when the event starts! Active monitoring and moderation are your first line of defense against disruption, technical hiccups, or security breaches.

- **Assign Live Monitoring Roles** - Designate team members to actively watch the attendee list, video feeds, screen shares, chat, and Q&A. Their goal is to spot and respond to anything unusual FAST.
- **Moderate in Real Time** - Enforce your Code of Conduct promptly and respectfully. Keep sessions on track by managing spam, abusive behavior, and off-topic chatter.
- **Train and Empower Your Moderators** – Make sure your mods are both trained and authorized to act quickly, whether that's muting a mic, disabling video, removing a disruptive attendee, or locking the meeting.
- **Watch Platform Performance** – Monitor system health and stay alert for service issues or vendor status updates. Early awareness helps minimize disruptions.

eventbuilder
enterprise virtual event services

INCIDENT RESPONSE PREPAREDNESS

Preparation is power. Having a virtual event-specific incident response plan (IRP) ensure you're equipped to handle the unexpected with confidence.



- **Develop a Virtual Event IRP** - Create or tailor an incident response plan specifically for live, online event environments. Generic IT plans won't cover the nuances.
- **Define the Response Team** - Assign clear roles and responsibilities, and maintain updated contact info so you can easily mobilize those resources quickly.
- **Build Scenario-Based Playbook** - Outline action steps for likely incidents like Zoombombing, platform outages, phishing attempts, or suspected data leaks. Knowing what to do ahead of time saves precious minutes.
- **Have Backup Communication Ready** - If your main platform goes down, how will you reach your attendees? Use pre-collected email lists, backup platforms or social media groups to stay connected.
- **Test and Refine the Plan** - Run tabletop exercises or simulations to test your team's readiness. These drills help surface gaps before the real thing does.

eventbuilder
enterprise virtual event services

POST-EVENT PROCEDURES

Your security obligations don't end when the event does. How you handle data and follow-up activities matters just as much as your live execution.

- **Securely Store Event Data** - Store everything in encrypted, access-controlled environments that align with your data protection policies, including recordings attendees lists, and chat transcripts.
- **Apply Retention and Deletion Policies** - Delete or anonymize personal data once your retention timeline expires. Stick to what you've promised and documented.
- **Complete Outstanding DSARs** - Ensure all data subject or consumer rights requests (access, deletion, corrections) have been addressed and documented properly.
- **Conduct a Post-Event Review** - Analyze logs, flag any issues, and gather internal feedback. If a security incident occurred, conduct a root cause analysis and update your plans accordingly.
- **Handle Follow-Up Responsibly** - When sending surveys or follow-up emails, honor consent and opt-out preferences. Use secure email platforms and verify recipient lists before sending.

eventbuilder
enterprise virtual event services

ACHIEVING SECURE AND COMPLIANT VIRTUAL EVENTS

Securing virtual events is more than a checklist item—it's a holistic process that blends strategic planning, platform expertise, and real-time responsiveness.

As threats evolve and expectations rise, virtual event security and compliance must become part of your organization's event DNA. Use this checklist as both a starting point and an ongoing guide to help you stay proactive, build attendee trust, and deliver professional, secure virtual experiences every time.

FEELING OVERWHELMED?

You're not alone! Covering every item on this checklist takes more than good intentions—it takes the right technology and an expert team to know what's needed and how to implement it effectively.

EventBuilder's platform, integrates with the secure infrastructure of Microsoft Teams, delivering the additional technical safeguards today's virtual events demand. Additionally, with our experienced Professional Services team by your side—you don't have to go it alone. We'll help you navigate compliance requirements, implement best practices, and create secure, engaging experiences that earn your attendee's trust.

LET US HELP YOU SECURE YOUR DIGITAL STAGE

...ARRANGE A CONSULTATION