



tag

BRAND SAFETY

BRAND SAFETY CERTIFIED

Guidelines
Version 4
July 2024



ABOUT THE BRAND SAFETY CERTIFIED PROGRAM

The mission of the TAG Brand Safety Certification is to significantly reduce the risk of the misplacement of advertising on digital media properties of all types, thereby upholding Brand Safety and protecting the integrity of digital advertising. TAG's Brand Safety Certified Program promotes the flow of advertising budgets to participants in digital advertising upholding an industry regulated framework for Brand Safety.

In order to enable companies to promote a brand safe environment, the TAG Brand Safety Certification Working Group maintains the Brand Safety Certified Guidelines. Companies that are shown to abide by the Brand Safety Certified Guidelines can achieve the Brand Safety Certified Seal and use the Seal to publicly communicate their commitment to minimizing ad misplacement and fostering an environment of trust in the marketplace.

ABOUT TAG

TAG (Trustworthy Accountability Group), is the leading global certification organization fighting criminal activity, promoting Brand Safety and increasing trust in the digital advertising industry. TAG's mission is to:

- Eliminate fraudulent traffic;
- Combat malware;
- Prevent internet piracy, and
- Promote brand safety and greater transparency in digital advertising.

TAG advances those initiatives by bringing companies across the digital advertising supply chain together to set the highest standards.

TAG is the first and only registered Information Sharing and Analysis Organization (ISAO) for the digital advertising industry.

To learn more about TAG, please visit www.tagtoday.net.

1. Executive Summary	4
2. Certification process	6
2.1. Application	7
2.1.a. Participation Fee	7
2.2. Qualification	7
2.3. Geographic Applicability of Certification	7
2.4. Method of Certification	8
2.5. Publication of Certification Status	8
2.5.a. Brand Safety Certification Seal	8
2.6. Continued Compliance	9
2.6.a. TAG Compliance Officer	9
2.6.b. Compliance Team	9
2.6.c. Training	9
2.6.d. Quarterly Internal Reviews	10
2.6.e. Internal Quarterly Reviews and Inclusion/Exclusion lists	10
2.6.f. Recertification	10
3. Covered Parties	11
3.1. Direct Buyers	12
3.2. Direct Sellers	12
3.3. Intermediaries	12
3.4. Content Verification Services	12
3.5. Anti-Piracy Service Providers	13
4. Certification Requirements	14
4.1. Requirements Tables	15
4.2. Complete TAG Registration and Be a TAG Member in Good Standing	16
4.3. Have a Designated TAG Compliance Officer	16
4.4. Complete a Brand Safety Certification Training Annually	16
4.5. Ensure that all new and updated digital advertising agreements adhere to Brand Safety and anti-piracy Requirements	16
4.5.a. Content Taxonomy	17
4.6. employ effective Ad Misplacement avoidance services and/or tools	17
4.7. Document Policies and Procedures Related to employing effective ad Misplacement avoidance services and/or tools	18
4.8. Employ Pirate Mobile App Detection And Removal	18
4.9. Employ Pirate Domain List DetectioN and Removal	18
4.10. Define and Identify Key Roles and Resources	19
4.11. Ensure Inclusion/Exclusion Lists Are ReviewEd Quarterly	19
4.12. Provide Effective Content Verification Services	19
4.12.a. Content Verification Requirements	19
4.13. provide effective Anti-Piracy services	20
4.13.a. Anti-Piracy Requirements	20
5. Allegations of Non-Compliance & Appeal	22
6. Appendix A	24
7. Appendix B	26



EXECUTIVE **SUMMARY**

No reputable brand wants their advertisement placed adjacent to highly objectionable content, including sites promoting fake news, inciting hate speech, or encouraging criminal behavior, such as sites that contain pirated content. At the same time, neither buyers nor sellers are well served by mechanistic processes that may inadvertently block placement on brand-appropriate sites.

The mission of the TAG Brand Safety Certified Program is to significantly reduce the risk of the misplacement of advertising on digital media of all types, thereby upholding Brand Safety and protecting the integrity of digital advertising.

The TAG Brand Safety Certified Program promotes the flow of advertising budgets to participants in digital advertising upholding an industry regulated framework for Brand Safety. The program serves the entire digital advertising supply chain by providing transparency, choice, and control for buyers – enabling them to buy advertising inventory with confidence and creating a Brand Safety framework for sellers that increases the value of certified sellers' inventory.

The background features abstract geometric shapes in shades of teal and light blue, primarily located in the top-left and bottom-right corners. These shapes consist of overlapping triangles and quadrilaterals, creating a modern, dynamic feel.

CERTIFICATION **PROCESS**

The TAG Brand Safety Certified Program is a voluntary self-regulatory digital advertising industry initiative. It represents the on-going process of defining and maintaining guidelines for promoting the flow of advertising budgets to participants in digital advertising upholding an industry regulated framework for Brand Safety and providing transparency to buyers.

TAG certifies companies at the entity level, rather than certifying a specific product or business line within a legal entity. To achieve the TAG Brand Safety Certified Seal, companies must show that all of its material operations related to ad monetization services within a particular geographic market are in compliance with the relevant requirements of the Certification's requirements.

2.1. APPLICATION

Before a company can apply for the Brand Safety Certified Seal, that company must first complete the process of becoming "TAG Registered" and enrolling in the Verified by TAG Program. Companies can learn more and apply for TAG Registration by contacting TAG at info@tagtoday.net or visiting www.tagtoday.net.

Once a company has been approved as "TAG Registered" and enrolled in the Verified by TAG Program, the company's designated TAG Compliance Officer may contact TAG directly to request enrollment in the Brand Safety Certified Program in order to begin the process for that company to achieve the Seal. In order to participate, a company's TAG membership must include access to that Program.

2.1.a. Participation Fee

There is an annual fee, which is encompassed in annual membership fees, for participation in the Brand Safety Certified Program.

2.2. QUALIFICATION

Any TAG member company that has been enrolled in the Verified by TAG Program and whose TAG membership includes participation in the Brand Safety Certified Program can participate in the Program and apply for the Seal.

Requirements to achieve the TAG Brand Safety Certified Seal differ according to a company's role in the digital advertising supply chain. These roles and requirements are outlined in Sections 3 and 4 of this document.

2.3. GEOGRAPHIC APPLICABILITY OF CERTIFICATION

The Brand Safety Certified Seal can be achieved in any geographic market. However, upon achieving certification, a company is only permitted to use the Brand Safety Certified Seal in the specific geographic markets in which TAG has found the company's operations to be in full compliance with the Brand Safety Certified Guidelines. Additionally, any use of the Seal must identify the geographic markets to which it applies.

Companies can choose to certify operations either by country (e.g. United States, United Kingdom), by region (e.g. North America, Europe), or globally. Companies must clearly state which option it is applying for certification in its application for the Brand Safety Certified Seal.

2.4. METHOD OF CERTIFICATION

Companies must apply to achieve the Brand Safety Certified Seal through independent validation. The certification method is recorded and displayed on www.tagtoday.net.

Certification through independent validation is obtained by the company inviting an independent auditor to review and validate that the company has achieved full compliance with the ***Brand Safety Certified Guidelines***, as well as a series of binding attestations from the company in which it attests to have achieved full compliance with the ***Brand Safety Certified Guidelines*** and that it will maintain compliance throughout the certification period. A validating company must be an approved auditing company that includes a specialty in digital media audits.

As independent validation is designed to provide external assurance, ensuring that all Brand Safety Certified roles and requirements are being met within the company's operations, technology and supporting documentation may take some time to examine. Examination time depends on several factors such as company operations maturity level, organization size and complexity and technology.

Independent validation will include examination of, but not limited to, the following:

- Job description of the TAG Compliance Officer.
- Training policy and procedures.
- Internal audit policies and procedures.
- Established policies and procedures related to internal control.
- Policies and procedures related to the requirements of the Brand Safety Certified Guidelines.
- Policies and procedures related to complaint handling/resolution to ensure compliance with the Brand Safety Certified Guidelines.
- Testing performed by the company as part of the internal quarterly review process.
- For Content Verification Services and Anti-Piracy Service Providers. Testing performed by the auditor to check the efficacy of disclosed capabilities.

Entities that wish to achieve the TAG Brand Safety Certified Seal through independent validation should have the validating company submit to TAG: ***the Independent Validation Attestation, the Application for TAG's Brand Safety Certified Seal***, signed TAG ***Compliance Officer Attestation*** and ***Business Executive Attestation***, as well as any supporting documents or materials required by the Program.

2.5. PUBLICATION OF CERTIFICATION STATUS

With training and consistent monitoring procedures in place, the company is certified when TAG determines the company to be in full compliance with the ***Brand Safety Certified Guidelines***, based on the required documentation submitted. TAG notifies the company of its certification status, and that certification status is posted to the TAG Registry. Upon certification, TAG sends Certification Seal materials to the company's designated TAG Compliance Officer for use in promoting the company's Brand Safety Certified Seal status.

2.5.a. Brand Safety Certification Seal

Companies that are shown to meet the ***Brand Safety Certified Guidelines*** requirements receive the Brand Safety Certified Seal and can use it to publicly communicate their commitment to promoting transparency and Brand Safety in the digital advertising supply chain.

2.6. CONTINUED COMPLIANCE

Companies that are shown to meet the requirements of the *Brand Safety Certified Guidelines* and achieve the Brand Safety Certified Seal must maintain compliance throughout the certification period and renew their compliance annually.

2.6.a. TAG Compliance Officer

Companies participating in the Brand Safety Certified Program must designate a qualified TAG Compliance Officer. This is usually done in the process of the company's application for TAG Registration, prior to participation in the Brand Safety Certified program.

The duties of a TAG Compliance Officer include:

- Serving as the primary point of contact between TAG and the company regarding all aspects of the company's TAG membership. This includes receipt of notice concerning any changes to TAG Certification program(s).
- Completing the required training modules for each TAG Certification program in which the company participates.
- Educating internal teams on the requirements of each TAG Certification program in which the company participates and notifying those internal teams of any changes.
- Overseeing the company's processes related to compliance with the requirements of each TAG Certification program in which the company participates.
- Facilitating internal review of the company's compliance with the requirements of each TAG certification program in which the company participates, including independent auditor review where appropriate.
- Taking on additional responsibilities applicable to each of the TAG programs in which the company participates (as appropriate).

The minimum qualifications for a TAG Compliance Officer include:

- Reporting relationships whereby compliance assessments are not influenced or biased by operations personnel being tested for compliance.
- Adequate technical training and proficiency in testing and assessing compliance.
- Adequate knowledge of the subject matter covered in each of the TAG Certification programs in which the company participates (i.e. advertising technology, various functions within the digital advertising supply chain, etc.).
- Adequate independence within the company to avoid conflicts of interest with regard to assessing compliance with TAG program requirements.

A TAG Compliance Officer does not need to hold a particular title or job description within the organization, as long as that individual has independence from sales and marketing functions.

The role of the TAG Compliance Officer is further described in the TAG Compliance Officer Role Description, available on www.tagtoday.net.

2.6.b. Compliance Team

While the only requirement to support compliance with the *Brand Safety Certified Guidelines* is the designation of a TAG Compliance Officer, it is also recommended that a company have in place a Compliance Team to assist in meeting and maintaining compliance with the *Brand Safety Certified Guidelines*.

2.6.c. Training

Brand Safety Certified training is required for the company's designated TAG Compliance Officer to complete annually. The Compliance Officer is encouraged to complete the online training,

after a company is enrolled in the Brand Safety Certified Program, in order for the company to achieve the Brand Safety Certified Seal. Training must be renewed on an annual basis in order for a company to maintain its Brand Safety Certified Seal from year to year.

TAG provides training through an online streaming video available through the TAG Member Portal, so that TAG Compliance Officers are able to obtain training regardless of geographic location or time-zone. TAG Compliance Officers can learn more and RSVP for training sessions by emailing info@tagtoday.net.

2.6.d. Quarterly Internal Reviews

Quarterly internal reviews ensure that a company that has been awarded the Brand Safety Certified Seal maintains full compliance with *Brand Safety Certified Guidelines* throughout the year.

The TAG Compliance Officer is responsible for overseeing quarterly internal reviews, which should ensure that:

- The *Brand Safety Certified Guidelines* are consistently and completely followed.
- Control activities discussed during *Brand Safety Certified Guidelines* training are formally documented.
- Potential violations of the *Brand Safety Certified Guidelines* are detected in a timely fashion.
- Appropriate corrective measures are taken in a timely fashion.

Internal reviews should also include a risk analysis of certain control functions to assess how much testing is needed to validate adherence. Also, actual testing of data, both quantitatively and qualitatively, should be used to validate that the existing control structure is designed correctly and operating effectively.

2.6.e. Internal Quarterly Reviews and Inclusion/Exclusion lists

Any company acting as a Buyer, Seller, or Intermediary must document their policies and procedures for maintaining their internal inclusion and /or exclusion lists, and must also execute those policies and procedures as part of their internal quarterly review process for companies with TAG certification requirements companies must provide to TAG the methodology for which keywords, key phrases, content categories, digital media properties, etc. are added to these lists and also how keywords, key phrases, content categories, digital media properties etc are removed from these lists.

2.6.f. Recertification

Certification is an on-going process and companies that achieve the Brand Safety Certified Seal must be recertified annually. Companies that achieve the Brand Safety Certified Seal must apply for recertification by January 31 each year in order to be considered for recertification in that calendar year. TAG sends recertification notifications to all certified companies prior to the start of the recertification submission period.

TAG reviews all applications for recertification and notifies companies whether they have achieved recertification by March 1.



COVERED **PARTIES**

The Brand Safety Certified Seal is applicable to several types of covered parties across the digital advertising supply chain:

- Direct Buyers
- Direct Sellers
- Intermediaries
- Content Verification (CV); and
- Anti-Piracy (AP) Service Providers.

Companies applying for the Brand Safety Certified Program must apply for the Seal under all relevant covered party categories, meeting the requirements relevant to each category, as described in Section 4.1.

3.1. DIRECT BUYERS

Direct Buyers are advertisers who own advertisements for placement in inventory on the publisher's websites or other media properties, or advertising agencies that directly represent such advertisers. A Direct Buyer is an advertiser – a brand company represented in the advertisements that it wants to place in the publisher's inventory. However, many brands hire an advertising agency to manage their advertising campaigns. A brand-appointed agency is also a Direct Buyer, except in cases it operates as an Intermediary. To qualify as a direct buyer, the agency must directly represent the advertiser.

3.2. DIRECT SELLERS

Direct Sellers are publishers that provide content to an audience. This type of Direct Seller sells ad space inventory on its websites or other media properties that offer value to advertisers depending on the size and demographics of the audience.

While a publisher may sell this inventory directly, larger publishers may appoint an agent to manage and sell this inventory. Such an agent is also a Direct Seller. To qualify as a Direct Seller, the agency must directly represent the publisher.

3.3. INTERMEDIARIES

An Intermediary is a company that owns and/or operates a technology or service that allows for the purchase of digital inventory for the purpose of ad placement.

Intermediaries include both Indirect Sellers and Indirect Buyers.

- An Intermediary may be an Indirect Seller in that it sells a Direct Seller's inventory.
- An Intermediary may be an Indirect Buyer in that it is qualified to assign a Direct Buyer's advertisements to a Direct Seller's inventory.

Any covered party that connects a Direct Seller to a Direct Buyer or an Indirect Seller through an ad technology layer or redirect is also an Intermediary.

3.4 CONTENT VERIFICATION SERVICES

Content Verification Services are entities that assist Direct Buyers, Direct Sellers and / or Intermediaries to protect brands against unnecessary risk, providing the capabilities to identify and/or control how best to select or avoid the context in which advertising appears. These

entities do not transact inventory but may be able to append to the creative payload or be declared in the campaign.

A primary service of a Content Verification Service is to assist Direct Buyers, Direct Sellers and/or intermediaries in protecting brands against seeing their advertising aligned with content that they deem inappropriate. They do this by classifying context and then ad alerting and/or blocking ads based on avoidance or target classification and/or categories.

3.5 ANTI-PIRACY SERVICE PROVIDERS

Anti-Piracy Service Providers are entities that assist Direct Buyers, Direct Sellers and / or Intermediaries to protect brands against unnecessary risk, providing the capability to identify and/or control how best to select or avoid the context in which advertising appears. These entities do not transact inventory but may be able to append to the creative payload or be declared in the campaign.

Anti-Piracy Service Providers are entities that assist Direct Buyers, Direct Sellers and / or Intermediaries to limit advertising on digital media properties that have a discernible risk of being associated with unauthorized dissemination of materials protected by copyright law and/or illegal dissemination of counterfeit goods.



CERTIFICATION **REQUIREMENTS**

Requirements to achieve the Brand Safety Certified Seal may differ according to a company's role in the digital advertising supply chain. To achieve the Brand Safety Certified Seal, an entity must meet relevant criteria based on the types of functions it undertakes.

To achieve the Brand Safety Certified Seal, a company must meet the requirements for all the categories in which it operates, according to the table below.

4.1. REQUIREMENTS TABLES

Requirements	Scope	Direct Buyer	Direct Seller	Intermediary	Content Verification Service	Anti-Piracy Service Provider
Complete TAG Registration and be a TAG Member in Good Standing	Administrative	√	√	√	√	√
Have a designated TAG Compliance Officer	Administrative	√	√	√	√	√
Complete Brand Safety Certified Training annually	Administrative	√	√	√	√	√
Ensure All Digital Advertising Agreements Adhere to Brand Safety and Anti- Piracy Requirements	Brand Safety and Anti-Piracy	√	√	√		
Employ Effective Ad Misplacement Avoidance Services and/or tools	Brand Safety and Anti-Piracy	√	√	√		
Document Policies and Procedures related to Employing Effective Ad Misplacement Avoidance Services and/or tools	Brand Safety and Anti-Piracy	√	√	√		
Employ Pirate Mobile Detection and Removal	Anti-Piracy	√		√		
Define and Identify Key Roles and Resources	Brand Safety and Anti-Piracy	√	√	√	√	√
Ensure Inclusion/Exclusion Lists are reviewed Quarterly	Brand Safety and Anti-Piracy	√	√	√		
Provide Effective Content Verification Services	Brand Safety				√	
Provide Effective Anti-Piracy Services	Anti-Piracy					√

4.2. COMPLETE TAG REGISTRATION AND BE A TAG MEMBER IN GOOD STANDING

To achieve the Brand Safety Certified seal, any participating company must first become a TAG member, completing the process of becoming “TAG Registered” and enrolling in the Verified by TAG Program (See Section 2.1). Companies can learn more and apply for TAG Registration by contacting TAG at info@tagtoday.net or visiting www.tagtoday.net. Companies seeking the Brand Safety Certification must also have an active TAG membership that includes participation in the Brand Safety Certification Program, have a valid TAG membership agreement in place, and be current on payment for all TAG membership fees.

4.3. HAVE A DESIGNATED TAG COMPLIANCE OFFICER

To achieve the Brand Safety Certified Seal, any participating company must have designated a qualified TAG Compliance Officer. The role of the TAG Compliance Officer is described in section 2.6.a of this document.

4.4. COMPLETE A BRAND SAFETY CERTIFICATION TRAINING ANNUALLY

To achieve the Brand Safety Certified Seal, any participating company’s designated TAG Compliance Officer is encouraged to complete the online training, after a company is enrolled in the Brand Safety Certification Program, as outlined in Section 2.6.c.

4.5. ENSURE THAT ALL NEW AND UPDATED DIGITAL ADVERTISING AGREEMENTS ADHERE TO BRAND SAFETY AND ANTI-PIRACY REQUIREMENTS

To achieve the Brand Safety Certified Seal, any participating company acting as a Direct Buyer, Direct Seller and/or Intermediary must ensure that new and updated agreements for digital advertising services adhere to the Brand Safety and Anti-Piracy Requirements listed below.

Depending on the covered party categories (see Section 3) into which a participating company falls, all participating companies must comply with the following requirements.

- Direct Buyers, Direct Sellers and Intermediaries must ensure that all monetizable actions conform to either a Primary Agreement or the specific terms and policies within an agreed or signed contract.
- Direct Buyers and Intermediaries must define the criteria to be met in order for digital advertising to be presented on digital media property(ies).
- Direct Buyers and Intermediaries must select an effective means to avoid ad misplacement, addressing both Brand Safety and anti-piracy.
 - Independently validated Content Verification services or Brand Safety Inclusion/Exclusion lists.
 - Independently validated Anti-Piracy services, or Anti-Piracy Inclusion/Exclusion Lists.
- Direct Buyers, Direct Sellers and Intermediaries must define the policies and procedures, used to monitor and demonstrate compliance with each of the applicable Brand Safety

and Anti-Piracy principles listed in this section, including but not limited to takedowns, make goods, reversals/clawbacks etc.

- Direct Sellers must provide an attestation that they own or have licensed the rights to all relevant content appearing on their owned and operated media properties.
- Direct Sellers must provide TAG with an attestation that the company does not block or unduly restrict the legitimate use of Content Validation and Anti-Piracy services (defined in Section 3.4 and 3.5). For this purpose, “legitimate use”, refers to the use of validating the content is not associated with issues of brand safety and /or piracy, as governed by terms agreed between the Direct Buyer and the Direct Seller.
- In the event that a Direct Seller has concerns with the use of such technologies extending beyond the purposes defined above as “legitimate use”, the Direct Seller will not be deemed out of compliance of the Brand Safety Certified Guidelines should it restrict or limit such technologies from being deployed on its digital properties for purposes beyond those defined above as “legitimate use”.

4.5.a. Content Taxonomy

Content taxonomies exist to create a common method for ensuring transparency and disclosure into the types of content that may be associated with digital advertising, empowering choice and brand-safety for advertisers.

Any participating company acting as a Direct Buyer, Intermediary, Vendor or Seller must employ the use of a TAG-recognized content taxonomy for defining and avoiding harmful content, as referenced in Appendix B.

- Any participating company acting as a Direct Buyer should implement a TAG-recognized content taxonomy to avoid the harmful content taxonomy floor as referenced in Appendix B. This must be accomplished using tools provided by Content Verification Services and/or robust methods of creating inclusion/exclusion lists. Sharing documentation, such as Terms of Service, Site Level Agreements, or other contractual agreements in place that demonstrate compliance with this requirement.
- Any participating company acting as a Direct Seller, Intermediary, and/or Vendor, should adopt and operationalize a TAG-recognized content taxonomy to ensure that the defined floor for harmful content as referenced in Appendix B. may be avoided.

4.6. EMPLOY EFFECTIVE AD MISPLACEMENT AVOIDANCE SERVICES AND/OR TOOLS

To achieve the Brand Safety Certified seal, any participating company acting as a Direct Buyer, Direct Seller and/or Intermediary must employ effective Ad Misplacement Avoidance Services and/or Tools across 100% of the monetizable transactions that the company handles. Employing effective Ad Misplacement Avoidance Services and Tools may be achieved through the use of one or more independently validated Content Verification and one or more independently validated Anti-Privacy services, or through the use of Brand Safety and Anti-Piracy Inclusion/Exclusion Lists, as defined in the company’s digital advertising agreements.

Direct Sellers will be required to disclose, upon request the following:

- Policies for the additional monitoring, detection, and management of risk against ad misplacement, such as the use of editorial codes,
- The means by which the company ensures that their media properties do not host or stream copyright infringing or counterfeit content.
- Attest that the company does not block or unduly restrict the legitimate use of Content Verification and Anti-Piracy services.

4.7. DOCUMENT POLICIES AND PROCEDURES RELATED TO EMPLOYING EFFECTIVE AD MISPLACEMENT AVOIDANCE SERVICES AND/OR TOOLS

To achieve the Brand Safety Certified Seal, any participating company acting as a Direct Buyer, Direct Seller and/or Intermediary must document the specific policies and procedures they have to minimize the risk of ad misplacement through the use of effective ad misplacement avoidance services and /or tools. These policies and procedures must include, but are not limited to:

- Identifying staff and/or tools/technology used to review and/or flag content as brand safe.
- Identifying staff and/or tools/technology used to review or flag content disclosing from media properties associated with piracy.
- Identifying and operationalizing technology and procedures used for the creation and ongoing maintenance of inclusion/exclusion lists for content as brand safe.

Participating companies should have an objective review and evaluation process for claims of erroneous designation or scoring or determination of those entities 'digital media properties or content contained within, as unsafe.

4.8. EMPLOY PIRATE MOBILE APP DETECTION AND REMOVAL

To achieve the Brand Safety Certified Seal, a participating company acting as a Direct Buyer and/or Intermediary must employ pirate mobile app filtering for all advertising displayed in a mobile app environment.

Use of TAG's Pirate Mobile App List is available to assist companies in meeting this requirement, but use of the tool is not required, nor does the use of the tool, in-and-of-itself, fulfill this requirement.

4.9. EMPLOY PIRATE DOMAIN LIST DETECTION AND REMOVAL

To achieve the Brand Safety Certified Seal, a participating company acting as a Direct Seller, Direct Buyer and/or Intermediary provider must employ pirate domain detection and removal for all digital advertising.

Use of TAG's Pirate Domain Exclusion List is available to assist companies in meeting this requirement, but use of the tool is not required, nor does the use of the tool, in-and-of-itself, fulfill this requirement.

4.10. DEFINE AND IDENTIFY KEY ROLES AND RESOURCES

To achieve the Brand Safety Certified Seal, any participating company acting as a Buyer, Seller, Vendor or Intermediary must define and identify the internal roles and resource(s) responsible for the responding to incidents of ad misplacement due to issues of brand safety and piracy on behalf of the company. Internal roles and resources are considered the personnel and/or team(s) responsible for responding to brand safety and piracy events, as well as tools utilized by those personnel and /or team(s) to identify, mitigate and /or manage inappropriate ad placement and piracy events.

Companies must also document the external resource(s) responsible for responding to incidents of ad misplacement due to issues of brand safety and piracy. External resources are considered the personnel and/or team(s) and or tool(s) with whom the identified internal resources utilize with regards to incidents of ad misplacement due to issues of brand safety and piracy. The list below defines which external resource(s) must be documented for each applicable Covered Party type the company fulfils.

- Direct Buyers must document the roles and responsible resource(s) with each of their vendor companies.
- Direct Sellers must document the roles and responsible resource(s) with their direct intermediary companies in the supply chain.
- Intermediaries must document the roles and responsible resource(s) with their buy-side and sell-side partners in the supply chain, as well as with their Content Verification and Piracy Vendor(s)
- Vendors must document the roles and responsible resource(s) for each client company for whom they are providing services as defined in Section(s) 3.4 and 3.5

Such responsible parties may include internal and external teams, provided that they demonstrate clear lines of communication across partners.

4.11. ENSURE INCLUSION/EXCLUSION LISTS ARE REVIEWED QUARTERLY

Any company acting as a Buyer, Seller, or Intermediary must document their policies and procedures for the maintenance of inclusion and/or exclusion lists and must also execute those policies and procedures as part of their internal quarterly review process for the compliance with TAG certification requirements. Companies must provide to TAG the methodology for which keywords, key-phrases, content categories, digital media properties are added to these lists, and also how keywords, key-phrases, content categories, digital media properties etc. are removed from these lists.

4.12. PROVIDE EFFECTIVE CONTENT VERIFICATION SERVICES

These requirements apply to products that address Brand Safety by classifying, reporting and in some cases blocking content deemed to be appropriate or inappropriate by an advertiser in both desktop and mobile environments. See appendix A. for mobile definition.

4.12.a. Content Verification Requirements

In order to achieve the Brand Safety Certified Seal, any participating company acting as a Content Verification Service must disclose all of the content verification requirements that their services are able to fulfill.

A Content Verification Service must provide brand suitability classifying, reporting, and, if applicable, blocking services at a property and content level. This will include, but will not be limited to, how they classify, report and/or block based on domain, sub-domain, alias, app name, source code, content, context, images, videos, audio, adjacency and dynamic content, e.g. UGC comments.

A Content Verification Service must provide tools and/or data that provide buyers and/or sellers with the information and/or controls to enable customized targeting of content deemed brand safe and avoidance of content deemed brand unsafe. This will include but will not be limited to what targeting options are offered, whether this be;

- lists of keywords
- the creation of custom categories, or
- taxonomy such as the IAB Tech Labs v.2.2 etc.

A Content Verification Service must disclose methodologies and controls employed to maintain property and content data quality. This will include but will not be limited to how the product handles minimum traffic thresholds, the frequency it classifies and reclassifies content, time thresholds for incorporating lists, and actions taken to minimize the impact on ad delivery e.g. latency born about by demand on the page.

A Content Verification Service must disclose instances where content verification is not possible. A Content Verification Service must have an objective review and evaluation process for any claims brought about for wrongful classification of content being brand unsafe.

4.13. PROVIDE EFFECTIVE ANTI-PIRACY SERVICES

These requirements apply to products that address anti-piracy by classifying, reporting and in some cases blocking content deemed to be a pirated content risk in both desktop and mobile environments. See appendix A for mobile definition.

4.13.a. Anti-Piracy Requirements

In order to achieve the Brand Safety Certified Seal, any participating company acting as an Anti-Piracy Service Provider must disclose all of the Anti-Piracy requirements their services are able to fulfill.

All Anti-Piracy Services must have protocols and capabilities to identify media properties that have a discernible risk of being associated with unauthorized dissemination of materials protected by copyright laws and/or illegal dissemination of counterfeit goods, and all must have an objective review and evaluation process for claims of erroneous designation or scoring or determination of those digital media properties, or content contained within, as entities associated with piracy.

Also, an Anti-Piracy Service Provider must be able to perform with proficiency at least one of the capabilities, from the list below and they must disclose to TAG all of the additional capabilities that they are able to fulfill.

- I. Have protocols and capabilities to prevent advertising spent on media properties that have been identified as having a discernible risk of being associated with unauthorized

dissemination of materials protected by copyright laws and/or illegal dissemination of counterfeit goods.

- II. Can provide or enable the provision of real-time solutions to effectively prevent ads appearing on pirate/counterfeit content, and have the ability to provide reporting, logs-of-activity, and other data that enable Intermediaries and Direct Buyers to attempt chargebacks/reversals should ads appear on pirate/counterfeit content.
- III. Have protocols and capabilities to detect identified pirate and counterfeit content being transacted fraudulently or deceptively (e.g., through the use of intermediary sites or other means to disguise their identity or purpose).
- IV. Have the ability to report on advertisements appearing on identified pirate and counterfeit media properties that are not in compliance with advertiser/agency instructions.



ALLEGATIONS OF
NON-
COMPLIANCE &
APPEAL

Companies that achieve the Brand Safety Certification Seal must meet and maintain compliance with the relevant requirements for the **Brand Safety Certification** throughout the certification period. Failure to comply can result in consequences, including but not limited to the loss of certification and use of the Brand Safety Certification Seal. Certified companies are permitted to review allegations of non-compliance, submit rebuttal evidence, seek review of decisions of non-compliance and appeal any final decision.

The formal process governing non-compliance can be found in TAG's **Due Process for Allegations of Non-Compliance and Appeal**, available on www.tagtoday.net

The page features a white background with large, abstract geometric shapes in teal and light blue in the corners. These shapes are composed of overlapping triangles and parallelograms, creating a modern, architectural feel. The teal shapes are darker and more prominent, while the light blue shapes are layered behind them, adding depth to the design.

APPENDIX

A

Mobile includes:

- Mobile Web – website content displayed within a mobile web browser or embedded browser.
- Mobile In-App – content within the native user interface of an application, so not within a mobile browser or an embedded browser.



APPENDIX **B**

The 11 “Sensitive Topics” content categories as defined by the IAB Tech Lab Content Taxonomy version 2.2, and at the “Floor” risk-rating.

For more information on the IAB Tech Lab Content Taxonomy v2.2, please visit:

https://iabtechlab.com/wp-content/uploads/2020/12/Implementation_Guide_for_Brand_Suitability_with_IABTechLab_Content_Taxonomy_2-2.pdf

- Adult & Explicit Sexual Content
- Arms & Ammunition
- Crime & Harmful Acts to Individuals and Society and Human Right Violations
- Death Injury, or Military Conflict
- Online Piracy
- Hate Speech & Acts of Aggression
- Obscenity and Profanity
- Illegal Drugs/Tobacco/E-Cigarettes/ Vaping/Alcohol
- Spam or Harmful Content
- Terrorism
- Sensitive Social Issues

The 12 “Brand Safety Floor” and Framework identified in consultation with industry experts and representatives of NGOs, please visit

<https://www.brandsafetyinstitute.com/resources/frameworks/brand-safety-floor-suitability>

- Adult & Explicit Sexual Content
- Arms & Ammunition
- Crime & Harmful Acts to Individuals and Society and Human Right Violations
- Death Injury, or Military Conflict
- Online Piracy
- Hate Speech & Acts of Aggression
- Obscenity and Profanity
- Illegal Drugs/Tobacco/E-Cigarettes/ Vaping/Alcohol
- Spam or Harmful Content
- Terrorism
- Sensitive Social Issues
- Misinformation



tag

tagtoday.net