

ESCORTIFYS

GLOBAL SAFETY, REPORTING & TAKEDOWN POLICY

Document 5 | Pre-Publication Final Draft

Purpose

This Policy explains how users, depicted persons, rights holders, affected persons, and other legitimate reporters can report safety, illegality, impersonation, privacy, image-rights, fraud, or other prohibited-content concerns to Escortifys, and how Escortifys may triage, restrict, investigate, remove, preserve, escalate, and review reported material.

Draft date: 22 August 2026 | Public effective date: [TO BE INSERTED AT LAUNCH]

Critical enforcement rule

When Escortifys confirms, for platform-enforcement purposes, that an account is responsible for minor/CSAM conduct, trafficking or coercion, non-consensual intimate material, or deliberate identity-verification fraud, the default outcome is permanent account termination rather than graduated warnings. A mere allegation or unverified report is not confirmation. Mandatory redress rights and correction of demonstrable error remain available where applicable.

Immediate danger

Escortifys is not an emergency service. If a person is in immediate danger, contact local emergency services or law enforcement first. A platform report should not be used as a substitute for urgent emergency assistance.

Contents

1. Scope and relationship to other policies
2. Who may report
3. What may be reported
4. Emergency and urgent-safety reports
5. Underage and child sexual abuse or exploitation reports
6. Trafficking, exploitation, coercion, and forced-participation reports
7. Non-consensual intimate material and voyeuristic content
8. Impersonation, stolen identity, and unauthorized listings
9. Stolen images, copyright, and image-rights complaints
10. Threats, stalking, extortion, doxxing, and harassment
11. Fraud, scams, account compromise, and verification fraud
12. Illegal or prohibited-service reports
13. Review and rating disputes
14. Restricted safety/fraud system disputes
15. How to submit a useful report
16. Do not redistribute illegal or abusive material
17. Reporter privacy and confidentiality
18. Good-faith reporting and no retaliation
19. Triage and priority handling
20. Temporary restrictions while a report is reviewed
21. Investigation and evidence assessment
22. Decision outcomes
23. Permanent termination for confirmed critical violations
24. Notice of decisions
25. Appeals, correction requests, and mandatory redress
26. Repeat offenders and circumvention
27. Evidence preservation and legal holds
28. Mandatory and permitted reporting to competent authorities
29. Government and law-enforcement requests
30. Cross-border and jurisdiction-specific takedown processes
31. No guarantee of removal time or outcome
32. Abuse of reporting systems
33. Records, auditability, and retention
34. Accessibility and reporting without an account
35. Changes and contact
- Appendix A. Report categories and information to collect
- Appendix B. Triage and enforcement matrix
- Appendix C. Internal legal and implementation notes - remove before publication

1. Scope and relationship to other policies

This Global Safety, Reporting & Takedown Policy applies to Provider Listings, profiles, images, video, text, external links, reviews and ratings if enabled, account information, verification submissions, commercial advertisements, messages if messaging is enabled, and other user-generated or user-associated material made available through Escortifys.

This Policy supplements the Terms of Service, Global Privacy Policy, Global Advertising & Listings Policy, Global Prohibited Content & Conduct Policy, and any applicable jurisdiction-specific rules. Where another policy or mandatory law imposes a stricter safety or removal requirement, the stricter requirement applies.

2. Who may report

Escortifys may accept reports from:

- a user or Provider with an Escortifys account;
- a person depicted, named, contacted, impersonated, threatened, harassed, or otherwise affected by content on the Platform;
- a parent, guardian, lawful representative, or authorized agent where appropriate;
- a copyright, trademark, privacy, publicity, or image-rights holder or authorized representative;
- a law-enforcement, regulatory, child-protection, anti-trafficking, emergency, or other competent authority acting within lawful authority;
- a trusted organization, hotline, victim-support organization, or other legitimate reporter;
- a person who does not have an Escortifys account, where an account should not reasonably be required to report the concern.

3. What may be reported

Reportable concerns include, without limitation:

- underage participation, age ambiguity, child sexual abuse or exploitation material, grooming, or sexual solicitation of a minor;
- trafficking, coercion, forced participation, debt bondage, document control, third-party exploitation, or unauthorized control of a Provider;
- non-consensual intimate material, voyeuristic media, hidden-camera material, leaked or hacked intimate media, or threats to publish intimate material;
- impersonation, unauthorized listing creation, stolen identity, stolen photographs, fake verification, or account takeover;
- credible threats, stalking, harassment, extortion, blackmail, doxxing, or unlawful surveillance;
- fraud, phishing, scams, deceptive payment demands, malware, credential theft, or account compromise;
- illegal or prohibited services, prohibited goods, unlawful recruitment, or content that violates Escortifys policies;
- copyright, trademark, privacy, publicity, confidentiality, or image-rights violations;
- abusive, false, retaliatory, or privacy-invasive reviews if reviews are enabled;
- a dispute about a restricted safety/fraud record if such a system is enabled;
- a moderation, verification, suspension, or takedown decision that is alleged to be based on error.

4. Emergency and urgent-safety reports

If a report indicates an immediate risk of death, serious physical harm, ongoing sexual violence, active child exploitation, kidnapping, trafficking, or another urgent emergency, the reporter should contact local emergency services or law enforcement first.

Escortifys may place content or an account on an immediate temporary safety hold while an urgent report is assessed. A temporary hold is a protective measure, not a final factual finding.

Where legally permitted and reasonably appropriate, Escortifys may preserve relevant records and make an emergency disclosure or referral to a competent authority. Emergency disclosures are not a substitute for ordinary legal process where no emergency exists.

5. Underage and child sexual abuse or exploitation reports

Reports involving a minor or apparent child sexual abuse or exploitation material receive the highest priority. Users should not download, save, screenshot, forward, email, re-upload, or otherwise redistribute suspected illegal child sexual abuse material in order to make a report.

- Provide the URL, listing/profile identifier, account name, date/time, and a concise description of the concern where possible.
- If the material appears to be hosted directly on Escortifys, identify its location without copying or redistributing it.
- If a child is in immediate danger, contact local police or emergency services immediately.
- Escortifys may immediately block or isolate the material, restrict the account, preserve legally required information, and follow mandatory child-safety reporting obligations.
- A confirmed account-level minor/CSAM violation is subject to permanent termination by default.

Do not send illegal images to support

A report about suspected child sexual abuse or exploitation material should ordinarily identify the content by URL, profile, listing, account, or other locator. Do not send copies of the suspected illegal material unless a lawful reporting process specifically requires or authorizes it.

6. Trafficking, exploitation, coercion, and forced-participation reports

Escortifys prioritizes reports that a Provider may be controlled, exploited, threatened, trafficked, forced, or deprived of independent control of their account, documents, money, communications, movements, or advertising.

Useful information may include:

- which account or listing is involved and who appears to control it;
- whether the depicted Provider can independently access, edit, pause, or delete the listing;
- threats, debt, document withholding, coercive housing, transportation, immigration, family, or violence-related pressure;
- evidence that another person controls the Provider's identity documents, phone, money, account credentials, or communications;
- a chronology of relevant events, where known, without embellishment or diagnosis.

A report is an allegation until reasonably assessed. Where Escortifys confirms trafficking, coercion, or forced participation for platform-enforcement purposes, permanent termination of the responsible account is the default outcome, subject to preservation and lawful referral requirements.

7. Non-consensual intimate material and voyeuristic content

A depicted person, authorized representative, or other legitimate reporter may request review and removal of intimate material believed to have been published, distributed, advertised, or made available without the required consent, or obtained through voyeurism, hacking, theft, or other unlawful means.

- Identify the specific image, video, profile, listing, URL, or account.
- State whether you are the depicted person or an authorized representative, if applicable.
- Explain briefly why the material is non-consensual, private, stolen, voyeuristic, hacked, or otherwise unauthorized.
- Escortifys may temporarily disable or limit access to the material while identity, consent, authenticity, or ownership is assessed.
- A confirmed account-level non-consensual intimate-material violation is subject to permanent termination by default.

8. Impersonation, stolen identity, and unauthorized listings

A person who believes they are being impersonated or advertised without authorization may request immediate review. Escortifys may require proportionate identity or control verification sufficient to distinguish the claimant from an impersonator without demanding unnecessary personal information.

- Unauthorized use of another person's name, photos, phone number, identity documents, verification result, or profile is prohibited.
- A listing may be hidden while a genuine ownership or identity dispute is resolved.
- An account that knowingly created an unauthorized listing may be terminated.
- Deliberate identity-verification fraud - including forged, stolen, synthetic, altered, or borrowed verification material - is a critical violation and, when confirmed, results in permanent termination by default.

9. Stolen images, copyright, and image-rights complaints

Image theft and intellectual-property complaints should identify the allegedly infringing material and the basis of the claimant's rights. Escortifys may request a source URL, original publication, ownership record, authorization, or other proportionate evidence.

Copyright notices that are subject to a jurisdiction-specific statutory notice process may require additional information and may carry statutory consequences for knowingly false statements. A separate Intellectual Property & Image Rights Policy may provide the detailed process.

10. Threats, stalking, extortion, doxxing, and harassment

Escortifys may immediately restrict content or accounts where a report presents a credible threat of violence, sexual violence, stalking, blackmail, sextortion, extortion, doxxing, or targeted harassment.

A report should preserve the reporter's own evidence where lawful and safe to do so, such as the relevant URL, account name, dates, message identifiers, or screenshots that do not themselves reproduce prohibited illegal material.

Where immediate danger exists, the reporter should contact local law enforcement or emergency services rather than waiting for platform review.

11. Fraud, scams, account compromise, and verification fraud

Reports of phishing, credential theft, fake support, account takeover, fraudulent payment demands, fake escrow or booking claims, stolen payment methods, malware, deceptive external links, or verification fraud may result in immediate security restrictions.

- Escortifys may reset credentials, revoke sessions, disable links, suspend accounts, require re-verification, or place account changes on hold.
- Victims of account compromise should not send passwords or authentication codes to support.
- Deliberate identity-verification fraud, once confirmed, is subject to permanent termination by default.
- Security restrictions may be applied before the full merits of a dispute are determined where necessary to prevent ongoing compromise.

12. Illegal or prohibited-service reports

A user may report a listing or account believed to advertise, solicit, promote, facilitate, or arrange illegal or otherwise prohibited conduct. Reports should identify the precise wording, field, link, media, or conduct at issue rather than making a generalized accusation.

Escortifys may remove content based on its own policies even where the reporter cannot prove a criminal offence. Platform moderation is not a criminal adjudication.

13. Review and rating disputes

If public reviews or ratings are enabled, a Provider may report a review that is alleged to be fake, retaliatory, extortionate, privacy-invasive, threatening, discriminatory, defamatory, spam, or otherwise prohibited.

Review moderation should distinguish criticism or an adverse opinion from a prohibited factual fabrication, threat, doxxing incident, or extortion attempt. A review is not removed merely because it is negative.

Reviews remain a legally gated feature. This section does not represent that public reviews are currently active.

14. Restricted safety/fraud system disputes

If Escortifys activates a restricted safety, fraud, or abuse-reporting system, affected persons must have a process to challenge material inaccuracies, mistaken identity, malicious reporting, or other qualifying errors where required by law or platform policy.

Operational details of restricted safety systems are not public. Such systems must not be treated as a public blacklist or as proof of criminal conduct. This section does not represent that any restricted provider-only safety-report feature is currently active.

15. How to submit a useful report

A useful report should provide, where reasonably available:

- the specific URL, listing ID, profile, image, review, account, link, or other content location;
- the report category and a concise factual description of the concern;
- the date and approximate time of the relevant event or discovery;
- the reporter's relationship to the issue, such as depicted person, rights holder, affected person, user, or witness;
- supporting non-illegal evidence that is reasonably necessary to assess the report;
- a safe contact method if follow-up is needed;
- whether immediate danger is alleged and whether emergency services have already been contacted.

Do not submit unnecessary government identifiers, medical records, intimate images, or unrelated private communications. Escortifys may request additional information only where reasonably needed for verification or decision-making.

16. Do not redistribute illegal or abusive material

Reporters must not create a second distribution event merely to prove that harmful content exists. Where content is illegal, intimate, exploitative, or highly sensitive, identify its location and describe the concern instead of forwarding the file unless a specific lawful process requires it.

This rule is particularly strict for suspected child sexual abuse or exploitation material, non-consensual intimate material, voyeuristic content, identity documents, and private personal data.

17. Reporter privacy and confidentiality

Escortifys will handle report information according to the Privacy Policy and applicable law. Reporter identity may be restricted from unnecessary disclosure, but Escortifys cannot promise absolute anonymity or confidentiality.

Information may need to be disclosed to the affected account, a court, regulator, law-enforcement agency, child-protection body, rights claimant, payment provider, infrastructure provider, or other competent entity where legally required or reasonably necessary and lawfully permitted.

Where notice to an affected account could create a material safety risk, compromise a lawful investigation, violate a legal prohibition, or expose a reporter unnecessarily, Escortifys may delay or limit notice where lawful.

18. Good-faith reporting and no retaliation

Good-faith reporting of a genuine safety or policy concern is permitted even if the report is ultimately not substantiated. Retaliation against a person for making a good-faith safety report is prohibited.

Knowingly false, fabricated, malicious, discriminatory, extortionate, or retaliatory reports may result in account restrictions or termination.

19. Triage and priority handling

Escortifys may triage reports by severity, immediacy, vulnerability, legal duty, confidence, content reach, repeat-offender history, and the risk that delay could cause further harm.

Priority	Illustrative reports	Default handling
Critical	Minor/CSAM; trafficking/coercion; active non-consensual intimate material; credible imminent threat; severe stalking/extortion; serious identity-verification fraud	Immediate priority queue; temporary restriction where warranted; human/safety/legal escalation
High	Impersonation; stolen intimate media; doxxing; account takeover; serious fraud; credible threats without immediate danger	Priority review; temporary restriction where warranted
Standard	General prohibited content; ordinary listing disputes; copyright/image-rights complaints; review disputes; spam	Normal moderation queue, subject to applicable legal deadlines

Escortifys does not promise a universal response time unless a specific legal obligation or published service commitment requires one. Response targets must match actual staffing and technical capability.

20. Temporary restrictions while a report is reviewed

To prevent continuing harm, Escortifys may temporarily hide, de-index, geoblock, blur, disable, freeze, or otherwise restrict content or an account while a report is assessed.

A temporary restriction is not a finding of guilt or criminal liability. It is a risk-control measure based on the information reasonably available at the time.

21. Investigation and evidence assessment

Escortifys may review relevant account records, verification records, content history, moderation logs, report history, security signals, non-public account information, and other information lawfully available to the Platform. It may seek information from the reporter or affected account where appropriate.

Reports are assessed as allegations unless supported by sufficient information for a platform decision. Escortifys does not diagnose, determine criminal guilt, or treat a private report as equivalent to a court finding.

A platform-enforcement finding may be made on a reasonable internal evidentiary basis that is appropriate to the safety and contractual decision being made; it need not await criminal charge, prosecution, or conviction.

22. Decision outcomes

A completed review may result in:

- no action because the report is unsupported, mistaken, outside scope, or does not violate the applicable rule;
- a request for correction, clarification, or additional verification;
- removal or restriction of a particular image, field, review, link, listing, or other content item;
- geoblocking, age gating, de-indexing, link disabling, or jurisdiction-specific restriction;
- temporary account hold, suspension, or re-verification;
- permanent account termination and anti-circumvention controls;
- correction of inaccurate restricted data where a correction mechanism applies;
- preservation of relevant evidence or implementation of a legal hold;
- referral or disclosure to a competent authority where required or lawfully appropriate.

23. Permanent termination for confirmed critical violations

The following confirmed account-level violations carry permanent account termination as the default platform consequence:

- minor/CSAM conduct or use of the Platform to facilitate child sexual abuse or exploitation;
- trafficking, coercion, forced participation, or knowing exploitation of another person;
- publishing, distributing, advertising, threatening to publish, or otherwise using non-consensual intimate material in violation of platform policy;
- deliberate identity-verification fraud, including knowingly using forged, stolen, synthetic, altered, borrowed, or another person's identity or verification material.

For this section, 'confirmed' means confirmed for platform-enforcement purposes after reasonable review of the available record. It does not mean that a criminal court has convicted the person. A report or accusation alone is not confirmation.

The default permanent-termination rule does not eliminate mandatory statutory appeal/redress rights or correction of demonstrable mistaken identity, administrative error, or materially unreliable evidence. Reinstatement is not required while a critical safety risk remains unresolved.

24. Notice of decisions

Where legally required or reasonably appropriate, Escortifys may notify the affected account of a moderation or takedown decision and provide a sufficiently clear reason. Notice may be delayed, limited, or withheld where law permits and notice could create a safety risk, expose a reporter, compromise an investigation, facilitate evasion, or disclose protected information.

Where applicable law requires a statement of reasons, complaint route, or other specific notice, Escortifys will use the required jurisdiction-specific process.

25. Appeals, correction requests, and mandatory redress

A user may request review of an eligible moderation decision where Escortifys offers an appeal or where applicable law requires one. Appeals should identify the decision, explain the claimed error, and provide relevant new or corrective information.

Appeal rights do not convert a safety hold into a right to immediate republication. Critical content may remain restricted while the appeal is decided.

A person alleging mistaken identity or factual inaccuracy in a restricted record may use the appropriate correction/dispute process if that feature exists.

26. Repeat offenders and circumvention

Escortifys may take reasonable measures to prevent a terminated or suspended user from evading enforcement through replacement accounts, new phone numbers, altered emails, different domains, reused images, devices, payment methods, proxies, another person's identity, or other circumvention techniques, subject to applicable law and privacy requirements.

27. Evidence preservation and legal holds

Escortifys may preserve relevant data when required by law, court order, preservation demand, child-safety reporting duty, legal hold, fraud investigation, safety investigation, or other lawful basis. Preservation is not the same as disclosure.

Preservation periods may differ by jurisdiction and legal process. Data that would not otherwise be retained should be destroyed when the preservation duty expires unless another lawful basis or order requires continued retention.

Highly sensitive preserved material should be subject to appropriate security and access controls. Exact technical controls are internal and are not disclosed in this public Policy.

28. Mandatory and permitted reporting to competent authorities

Escortifys will make reports or notifications when applicable law requires it. Escortifys may also make a voluntary report or disclosure where applicable law permits it and Escortifys reasonably considers the disclosure appropriate to address a serious safety risk, trafficking concern, child-safety concern, credible threat, fraud, or other serious unlawful activity.

The existence of a report to an authority does not itself establish that the reported person committed an offence. Escortifys should preserve the distinction between an allegation, a platform finding, and a governmental or judicial determination.

29. Government and law-enforcement requests

Requests from police, regulators, courts, or other authorities for non-public user information are handled under the separate Law Enforcement & Government Requests Policy. Informal official interest does not automatically entitle an authority to private user data.

Escortifys may verify the requesting authority, jurisdiction, legal basis, scope, account identifiers, time period, and form of process; seek clarification; preserve data when legally required; disclose only responsive information; and challenge or narrow defective or overbroad demands where legally available and appropriate.

30. Cross-border and jurisdiction-specific takedown processes

Escortifys is global, and reporting, removal, notice, preservation, appeal, and regulator-response duties differ by location. Escortifys may use regional workflows where required, including jurisdiction-specific forms, complaint rights, regulatory deadlines, trusted-notifier channels, statements of reasons, age/content controls, or mandatory reporting.

A regulatory or court removal notice that is legally binding on Escortifys will be handled according to its terms and applicable law.

31. No guarantee of removal time or outcome

Escortifys aims to address credible safety reports promptly, but does not promise that every report will result in removal, account termination, law-enforcement referral, or a particular response time unless applicable law or an express published commitment requires it.

The complexity of identity verification, consent disputes, cross-border law, evidence quality, urgent-safety obligations, technical dependencies, and lawful-process requirements can affect the outcome and timing.

32. Abuse of reporting systems

The reporting system must not be used to silence criticism, harass a competitor, expose a user, manufacture a safety record, pressure someone for money or services, retaliate after a dispute, or create false evidence.

Knowingly false or malicious reports may result in restriction or termination. This does not punish a good-faith reporter merely because a concern cannot ultimately be substantiated.

33. Records, auditability, and retention

Escortifys may maintain audit records of reports, moderation actions, decision reasons, appeals, preservation actions, authority referrals, verification disputes, and related safety activity for security, accountability, legal compliance, dispute handling, and abuse prevention.

Retention should be limited to what is reasonably necessary for the stated purpose and any legal requirement. Exact retention periods are governed by the Privacy Policy, internal retention schedule, legal holds, and jurisdiction-specific obligations.

34. Accessibility and reporting without an account

Safety and illegal-content reporting should be reasonably accessible and should not depend on maintaining a paid account. Affected persons should have a way to submit legitimate reports even where they are not Escortifys users.

Reporting forms should use clear categories, accessible controls, and plain-language instructions. Where practical, Escortifys should provide an alternative contact route for a person who cannot use the ordinary form.

35. Changes and contact

Escortifys may update this Policy to reflect legal developments, safety threats, platform changes, regulator requirements, moderation experience, or geographic expansion. Material changes will be communicated where applicable law requires it.

Platform: Escortifys.

General safety reporting: [TO BE INSERTED]

Urgent safety reporting: [TO BE INSERTED]

Impersonation / image-rights / takedown contact: [TO BE INSERTED]

Legal notices: [TO BE INSERTED]

Operator, controller, merchant, service-address, or similar particulars are disclosed where applicable law requires proactive disclosure and may otherwise be provided in response to an appropriate request.

Appendix A - Report categories and information to collect

Category	Core information	Handling note
Underage / CSAM	URL/listing/account locator; age concern; date/time; immediate-danger status	Do not request or accept unnecessary copies of suspected illegal material
Trafficking / coercion	Account/listing; person affected; control/coercion indicators; chronology; urgent danger	Avoid diagnosis; record observable facts and source
NCII / voyeurism	Specific media; depicted person/representative status; consent/privacy basis; source	Minimize copying; restrict access
Impersonation	Profile/listing; claimant identity/control evidence; source media/account	Proportionate verification only
Stolen images / IP	Specific content; original source; ownership/authorization basis	Route statutory notices to IP process where required
Threat / stalking / extortion	Account; dates; messages/URLs; nature of threat; immediate danger	Emergency-service reminder; preserve relevant records
Fraud / compromise	Account; link/domain; payment or login event; timestamps; security indicators	Never ask for passwords/authentication codes
Review dispute	Review ID; exact challenged statement; category of violation; supporting evidence	Negative opinion alone is not a takedown basis
General policy violation	Specific listing/content; policy category; concise explanation	Avoid vague 'illegal' reports without particulars

Appendix B - Triage and enforcement matrix

Class	Examples	Default response
Critical - immediate safety	Minor/CSAM; trafficking/coercion; credible imminent threat; active NCII; severe extortion/stalking	Immediate priority hold where warranted; human/safety/legal review; mandatory/permitted reporting analysis
Critical - confirmed account violation	Confirmed minor/CSAM; trafficking/coercion; NCII; deliberate identity-verification fraud	Permanent account termination by default; evidence preservation; anti-circumvention; authority reporting where required/appropriate
High	Impersonation; account compromise; doxxing; stolen intimate media; serious fraud; credible non-imminent threat	Priority restriction/review; verification; removal/suspension as warranted
Standard	Spam; duplicates; ordinary prohibited content; general IP/image-rights issue; review dispute	Normal moderation queue; correct/remove/restrict/appeal as applicable

Appendix C - Internal legal and implementation notes

INTERNAL - REMOVE BEFORE PUBLIC POSTING

This appendix records research, implementation gates, and jurisdiction-specific operating requirements. It should not appear in the final public web version.

C1. Project-record requirements carried into this Policy

- Project planning expressly calls for Report Listing, Report Image, Takedown Request, Impersonation Report, Verification Dispute, Review Dispute, legal-review flags, public-export controls, audit logs for moderation, retention/deletion rules, upload metadata stripping, secure-storage planning, consent logging, age acknowledgment, terms/privacy acceptance tracking, and a clear law-enforcement/takedown process.
- Public provider reviews and restricted provider-only safety reports remain legal-review-gated features and are not assumed to be live.
- The private safety system, if enabled, must not be a public blacklist; it requires moderation, structured categories, false-report penalties, retention limits, audit logs, correction/dispute/escalation, and no automatic banning from one report.
- Current project planning does not confirm live payments, messaging, booking, review submission, or safety-report submission.

C2. Canada - mandatory child-safety reporting

An Act respecting the mandatory reporting of Internet child sexual abuse and exploitation material by persons who provide an Internet service defines an 'Internet service' to include Internet access, Internet content hosting, or electronic mail. Section 2 requires a provider advised of an IP address or URL where child sexual abuse and exploitation material may be publicly available to report the address/URL to the organization designated by regulation as soon as feasible. The Regulations designate the Canadian Centre for Child Protection.

Section 3 requires a person providing an Internet service to notify police as soon as feasible where there are reasonable grounds to believe the service is being or has been used to commit a child sexual abuse and exploitation material offence. Section 4 requires preservation of related computer data for 21 days after a section 3 notification, followed by destruction of data outside the ordinary retention course unless another judicial order requires preservation. Regulation 12 requires the preserved copy to be kept in a secure offline location.

Operational consequence: the CSAM workflow must distinguish an externally hosted URL/IP report from a belief that Escortify itself has been used to commit the offence, and must implement the correct Cybertip.ca / police / preservation path. Do not rely on a generic 'may report' clause.

C3. United States - CyberTipline provider reporting

18 U.S.C. 2258A requires covered providers, as soon as reasonably possible after obtaining actual knowledge of facts or circumstances from which there is an apparent violation of specified federal child-exploitation offences, to make a report to NCMEC's CyberTipline. Current federal law also contains preservation and security requirements associated with provider reports. Exact applicability and preservation periods must be verified in the U.S. launch review.

Operational consequence: U.S.-linked child-safety reports require a jurisdiction-aware workflow; do not assume the Canadian Cybertip.ca procedure satisfies U.S. obligations.

C4. United Kingdom - reporting, complaints, and CSEA duty

Ofcom's current Online Safety Act guidance states that in-scope user-to-user services must allow users and affected persons to easily report illegal content and operate a complaints procedure. Ofcom has already taken enforcement action in 2026 concerning failures in reporting and complaints duties.

Ofcom also states that, from 7 April 2026, regulated user-to-user service providers must report detected and unreported child sexual exploitation and abuse content to the National Crime Agency; providers outside the UK are subject to the reporting duty for UK-linked CSEA content where the statutory scope is met.

Operational consequence: the UK flow must be separately mapped before launch, including illegal-content risk assessment, reporting, complaint access, recordkeeping, and CSEA reporting.

C5. European Union / EEA - DSA notice and action

Digital Services Act Article 16 requires covered hosting services to provide mechanisms allowing individuals or entities to notify specific allegedly illegal content. Where electronic contact information is provided, the service must confirm receipt and notify the reporter of its decision and redress possibilities. Notices must be processed in a timely, diligent, non-arbitrary, and objective manner. Article 17 requires clear and specific reasons for certain restrictions imposed because content is illegal or incompatible with platform terms.

Operational consequence: EU report records should include reporter/contact status, exact content locator, alleged legal/policy basis, receipt time, review action, automated-tool involvement, decision, reason, notice time, and redress route.

C6. Australia - image-based abuse removal

Australia's eSafety Image-Based Abuse Scheme permits removal notices requiring a relevant service or hosting provider to take reasonable steps to remove or cease hosting specified intimate images, ordinarily within 24 hours or a longer period specified in the notice. Non-compliance can attract enforcement consequences.

Operational consequence: Australian regulator notices require a dedicated legal intake route, timestamped handling, and an ability to disable identified content promptly.

C7. Comparator lesson - Locanto

Locanto's current Safety Center provides separate flagging for ads and images, conversation abuse reporting, user/ad blocking, phone verification, automated and human moderation, restricted-term filters, direct support, and law-enforcement collaboration. It states that reports may concern harmful conduct on or off the platform and that its team may remove ads or ban users after review.

Escortifys should borrow the accessible reporting architecture but maintain a tighter critical-safety escalation model because adult directory listings are the central product risk surface.

C8. Implementation requirements before public launch

- Create public Report Listing and Report Image controls on every live listing/media item.
- Create a non-account reporting route for depicted persons, impersonation victims, rights holders, and affected persons.
- Create dedicated report categories for underage/CSAM, trafficking/coercion, NCII/voyeurism, impersonation, threat/stalking/extortion, doxxing/privacy, fraud/compromise, stolen media/IP, illegal content/service, and other.
- Do not permit reporters to upload suspected CSAM through an ordinary evidence field.
- Create immediate-safety and ordinary moderation queues with clear escalation ownership.
- Implement the user's approved rule: confirmed minor/CSAM, trafficking/coercion, NCII, and deliberate identity-verification fraud result in permanent termination by default.
- Do not add a new technical restriction on staff/moderator provider-contact access at this stage; current access design remains unchanged pending later review.
- Implement audit logs for report receipt, temporary restriction, evidence preservation, decision, reason, notice, appeal, reinstatement, authority referral, and legal-process activity.
- Map Canada, United States, United Kingdom, EU/EEA, Australia, and each additional launch jurisdiction before enabling live listings.
- Finalize retention schedules for report evidence, audit logs, critical-safety records, and legal holds.
- Build an authority/referral directory with jurisdiction-specific police, child-safety, anti-trafficking, regulator, and emergency channels.
- Finalize public safety, urgent-safety, impersonation/takedown, and legal contact channels.
- Do not promise 24/7 human response until staffing actually supports it.
- Remove this internal appendix from the public web version after implementation and legal review.

C9. Official sources reviewed

- Canada: An Act respecting the mandatory reporting of Internet child sexual abuse and exploitation material by persons who provide an Internet service, S.C. 2011, c. 4, ss. 1-4; Internet Child Pornography Reporting Regulations, SOR/2011-292, including ss. 2 and 12; Cybertip.ca mandatory-reporting guidance.
- Canada: Criminal Code, R.S.C. 1985, c. C-46, ss. 162 and 162.1 (voyeurism and non-consensual publication of intimate images).
- United States: 18 U.S.C. 2258A (provider reporting requirements to NCMEC CyberTipline).
- European Union: Regulation (EU) 2022/2065 (Digital Services Act), Articles 16 and 17.
- United Kingdom: Ofcom, Illegal Content Duties under the Online Safety Act; Ofcom 2026 enforcement materials; Ofcom roadmap noting the CSEA reporting duty effective 7 April 2026 for regulated user-to-user services.
- Australia: eSafety Commissioner, Image-Based Abuse Scheme regulatory guidance on removal notices.
- Comparator: Locanto Safety Center (current public reporting, moderation, verification, blocking, and safety architecture).

Publication status

Document 5 is substantively complete as a global baseline. Before public posting, implement the reporting routes, critical-safety escalation, jurisdiction-specific mandatory-reporting workflows, audit logs, retention schedule, public contact channels, and any proactive legal-identity disclosures required by applicable law. Then remove Appendix C.