

# Best Practices for Online Identity Trust and Safety

7 Key Principles for Protecting Consumers  
and Preserving Business With Trusted Identities

**pipl.**<sup>®</sup>

## Identity Is an Essential Component of Trust and Safety

Online engagement is a snowball that has been rolling downhill since the very beginning of the internet. It just keeps getting bigger and building more momentum. It has transformed how business is done, to the benefit of digital consumers and the organizations providing online products and services.

But online interactions come with risk. Not all digital consumers act with good intentions. It's up to online organizations to protect their users and defend their platforms from abusive, harmful and fraudulent interactions that can damage brand reputation and lead to significant losses. With the rising global imperative to create a safer and more trustworthy internet, it's vital that companies embrace online trust and safety practices.

At the core of trust in online engagements is digital identity verification. And at the core of identity verification is identity trust. If a user's identity can't be verified, how can that user be trusted? Even with verified identities, it's even more important to establish that the individual behind the identity can be trusted. This guide provides best practices any organization can follow to develop effective trust and safety initiatives to protect their platform and their users.



increase in global  
internet users the  
past year


*DataReportal*

# 1 Assemble and Empower a Leadership Team

Establishing online trust and safety as a key priority for your business requires executive alignment and visibility across the organization. Successful trust and safety programs need full representation at the highest levels of an organization and allocation for a recurring budget.

Install executive-level leadership with oversight of a dedicated trust and safety team. Comprised of individuals with diverse expertise, the team will own the development, implementation and maintenance of an organization's trust and safety policy. The team should be consulted on any emerging trust and safety issues and be accountable for the overall performance of the organization's trust and safety initiatives.

Successful trust and safety programs require collaboration across the organization. Review and intervention from highly skilled and trained human decision makers is imperative when dealing with matters relating to abusive, deceptive or threatening human behavior. Digital safety cuts across disciplines and can involve product, user experience and compliance teams. Establish a cross-functional team to ensure your policies are applied consistently across the organization. Automated detection of trustworthy identities will also streamline the detection and immediate removal of fraudulent signups, fake reviews and other violations. This team should be supported with continuing training on the complex and evolving nature of trust and safety and the tools and resources necessary to maintain efficacy.

A photograph of two men in an office environment. One man, with a beard and wearing a white shirt, is sitting at a desk and looking towards the other man. The second man, older with glasses and a beard, is wearing a blue shirt and is partially visible on the right side of the frame. They appear to be in a meeting or collaborative work session. The background shows office cubicles and windows with blinds.

**“Recognize that user safety is a highest-order, company-wide initiative.”**

*Oasis Consortium*

## 2 Establish Foundational Policy and Protocol

Formalize the governing rules and appropriate procedures into an official policy that defines the scope of digital trust and safety initiatives within the organization. Details of the policy pertaining to users should be included in the organization's terms of service or another means of highly visible communication with consumers. And the policy should undergo regular review by an inclusive group of stakeholders for necessary updates to maintain relevance as the online trust and safety landscape evolves.

Digital trust and safety policy should:

- Encompass roles and responsibilities of all internal and external stakeholders
- Outline the rules of engagement for online interactions
- Include privacy and data security requirements
- Define clear expectations for what is and is not a trusted online identity and trusted engagement
- Conform to the boundaries of relevant legislation (nationally and globally), trust and safety association recommendations and internal compliance requirements
- Refine based on regional cultural norms, varied socio-economic backgrounds and the diversity of the online audience

**“There is no one-size-fits-all approach to handling online content and associated behavioral risks.”**

*Digital Trust & Safety Partnership*

## 3 Identify Risk and Assess Opportunities for Trust

There is some level of risk inherent in any online endeavor. Businesses transacting online must proactively identify potential threats to the business and its consumers from online abusers, scammers and fraudsters. Product teams should anticipate vulnerabilities and prepare to minimize them from the earliest stages of user engagement and throughout product launch and update cycles. Community guidelines should be prominently displayed, and there should be a process for users to report abuses. Many violations go unreported, so it is important to deploy tools to detect bad actors and monitor online interactions and routinely review and update risk models. Less risk leads to an improved customer experience and stronger business outcomes.

It's also beneficial to assess opportunities where prioritizing seamless engagement for trusted consumers will help balance out the introduction of friction to mitigate risk. Safe, frictionless experiences improve usability and enhance consumer confidence levels in the organization as a trusted, safety-minded brand.

41%

of U.S. adults have personally experienced online harassment

*Pew Research Center*

## 4 Pursue External Partnerships

Online trust and safety is certain to grow in scope and evolve in response to shifting trends and patterns of global internet usage. Organizations should collaborate with peer communities and third-party experts as well as seek partnerships with experienced vendors in order to keep up with current industry standards and consumer demands. These partnerships provide access to invaluable research and educational materials to guide product updates, policy decisions and user communications. Some of the world's most prominent online companies have joined dedicated internet safety organizations including the Trust and Safety Professional Association, the Brand Safety Institute, the Digital Trust & Safety Partnership, the Information Security Forum, the International Association of Privacy Professionals, the Oasis Consortium, the Trustworthy Accountability Group and others.

From an operational standpoint, working with outside technology vendors can enhance in-house resources with innovative technology and experienced counsel. AI-based technology can streamline content review while identity trust solutions can assess the identity behind the content, increasing the speed and accuracy of moderation efforts. Outside vendors should be vetted for compliance with privacy and security policies to ensure that they will protect your data and your online community. Third-party vendors are often the weak link in the security chain introducing added risk, so privacy and security requirements should be part of your vendor contracts.

**“Risks change over time and so approaches to mitigating them must also have room to evolve.”**

*Digital Trust & Safety Partnership*

## 5 Enforce Policy and Demonstrate Accountability

Online products and services are as varied as the communities that engage with them, and policy enforcement must be tailored accordingly. However, in all instances, enforcement should be fair and consistent for everyone. Enforcement roles should be clearly defined by function: reporting, reviewing, escalating, etc. Organizations should install formalized, role-specific training programs as well as wellness initiatives for team members who may be exposed to objectionable and abusive behavior as part of their involvement with content moderation protocol. Set expectations for response times and corrective actions to be taken based on risk tolerance. The nature of a business's online interactions may merit establishing a relationship with law enforcement—online safety threats can unfortunately portend offline threats to an individual's physical safety. Organizations have an obligation to notify the appropriate agencies in certain circumstances and in accordance with local government regulations. There should be an appeals process to address disputed enforcements.

An identity trust solution can enhance the enforcement team's detection and management of policy violations and increase confidence in decisioning. Organizations also should regularly engage with peer communities, researchers and industry partners to exchange knowledge of emerging trends, patterns and other mutually beneficial information to ensure risk models are kept current.

**“Users report only a fraction of violations. Deploy technology that can proactively detect a high proportion of harmful behaviors.”**

*Oasis Consortium*

## 6 Measure and Evaluate Progress

Set and measure against key benchmarks (e.g., violations reported, moderations requested, enforcements taken, automation volume) to evaluate the performance of the organization's online trust and safety initiatives. Regularly audit data and maintain meticulous record-keeping practices to aid in reporting. Analyze results to determine where progress has been made, improvement is needed and new opportunities for process innovation exist. In addition to evaluating operational efficacy, also consider the ongoing consumer impacts from content- and conduct-related moderation.

Compare organizational performance against industry standard metrics and solicit feedback from peer communities and third-party experts. Apply what's been learned to inform future updates to products and services as well as revisions to trust and safety policy and protocol.

90%  
of Americans say  
people being harassed  
or bullied online is a  
problem

*Pew Research Center*



# 7 Communicate Activities and Results

Transparent communication about your trust and safety program is a crucial way for your organization to show commitment to protecting online trust and safety. Maintain a regular frequency of transparent communication and include all internal and external stakeholders, including consumers. Outreach may also extend to peer communities, academic researchers and the public sector.

Messaging may take the form of performance data reports, notices of policy violations, warnings about potential threats, updates to policy, in-situ indicators within the product that are pertinent for consumers and other easily accessible channels of information sharing. Many large technology companies issue regular transparency statements to report on the performance of their security and privacy programs. Open communication with an educational purpose will engender a stronger sense of trust in the organization from key audiences and may encourage beneficial feedback.

79%

of Americans say social media companies are doing only a fair or poor job of addressing online harassment

*Pew Research Center*



# Identity Is at the Core of Trust

Pipl is the identity trust company. Our solutions enable organizations to identify trustworthy users, customers, partners and followers so that they can enhance their digital trust and safety initiatives. We're ready to show you how to implement trust in the ways that matter most to your organization.

Visit [pipl.com](https://pipl.com) to learn more.

.....

“Digital 2022: Global Overview Report,” DataReportal

“2022 Global Digital Fraud Trends Report,” TransUnion

“The State of Online Harassment,” Pew Research Center

“Best Practices Framework,” Digital Trust & Safety Partnership

“User Safety Standards for Our Digital Future,” Oasis Consortium

“Establishing Trust And Safety In Online Communities,” Forbes

## ABOUT PIPL

Pipl is the identity trust company. We make sure no one pretends to be you. We use multivariate linking to establish deep connections among more than 28 billion unique identifiers—email, mobile phone, social media and other data that spans the globe. Then we look at the big picture to derive identity trust. Our solutions allow organizations to provide frictionless customer experiences and establish trust across the consumer lifecycle. For more information, visit [pipl.com](https://pipl.com).

