XRSI

XR Safety Initiative

www.xrsi.org

EXTEND REALITY WITH AWARENESS

XR Safety and Privacy Guide for Artists

CYBER-XR COALITION

ARTIZEN

RH1 READY HACKER 1

EXTEND REALITY WITH AWARENESS!
XR Safety and Privacy Guide for Artists
DECEMBER 2020

Acknowledgements

Kavya Pearlman
XRSI

Marco Magnano
XRSI / Ready Hacker 1

Ryan Wegner
Ready Hacker 1

Nancy Baker Cahill
4th Wall

Andrea Kim
The Cyber XR Coalition

Alina Kadlubsky
The Cyber XR Coalition

Vandana Verma Sehgal
The Cyber XR Coalition

Michaela Ternasky-Holland
Activist Lens Grant

Jesse Damiani
Activist Lens Grant

René Pinnell
Artizen

*Cover designed by **Alina Kadlubsky***
*Design by **Marco Magnano** and **Alina Kadlubsky***

TABLE OF CONTENTS

Executive Summary 4

Chapter 1: Basic Cyber Hygiene Tips to Safely Extend Realities 5

Password Manager 6

Multi-Factor Authentication 7

Social Engineering 8

Malware and Botnets 9

Identity Management 10

Ransomware 11

Update your Systems and Browsers 12

Intellectual Property 13

Virtual Private Network 14

Maintain Backups 15

Chapter 2: Advanced Privacy and Security Enhancing Tips 16

Trust and Safety in the XR Domain 17

Make Future Truly Private with the XRSI Privacy Framework v 1.0 19

Focus Areas Overview 20

EXECUTIVE SUMMARY

Advances in immersive media are transforming storytelling into **story-living.**

Immersive media is no longer a "shiny new toy." Due to the catalyzing event of COVID-19 in 2020, it has already begun **changing the world** for the better by bringing people closer together across faith, race, class, gender, and ability. When it comes to advanced technologies, what is life-enhancing can also be **life-threatening**. The new worlds that we are building on top of our perceived reality bring along privacy and security risks. As we head for the mass adoption of these technologies and advancements, the risk awareness and mitigation are remarkably lacking in this domain. We are at a significant cross-section where the artists and media community needs **concrete guidance** and genuinely understand and carry out their share of security and privacy responsibilities.

This guide serves all of the artist and media communities. However, it zooms in on the subject of privacy and security for Individual creators, creative collaborators, and artistic developers. No matter which role you play, this guide can be used to ensure the key privacy and security considerations are taken into account during the design of XR products and experiences. Early adoption of these practices will help limit potential cybersecurity and privacy threats.

Taking privacy and security into consideration might not be a part of the natural creative process. However, it is essential to pay attention to these aspects when designing and developing. These proactive actions protect the artists themselves and the audience that may potentially interact with the art or enter into the same thought space as the one intended by the artist. Today's artists and developers are setting a precedent that will be followed by generations. Therefore we must get it right to create a safe and trustworthy ecosystem.

Many emerging technologies encounter what is known as the Collingridge dilemma: it is hard to predict the various impacts of a technology until it is extensively developed and widely used, but by then it is almost impossible to control or change. While we may not account for all the unintended consequences, we know that we need to pay attention to data protection and privacy. While these technologies present new ways to create wonderful new realities, we should also keep in mind how they can be used for repression, surveillance, propaganda, sow division, and how we risk losing privacy and control without adequate awareness and proactive actions over our own data and networks.

CHAPTER 1

BASIC CYBER HYGIENE TIPS TO **SAFELY EXTEND REALITIES**

Everyone can use these resources and tips to secure your online accounts and digital devices better and keep your data safe, whether you are an XR artist or not.

Password Manager

Lockdown Your accounts

Weak passwords or passwords shared between accounts can lead to compromises and account takeovers. A passphrase is a preferred alternative to keep your accounts secure. A passphrase can be sentences or phrases you like to think about and are easy to remember (for example, “I love electronic music.”). A strong passphrase is a sentence that is at least 12 characters long. While it used to be necessary to memorize a series of complex passwords to remain secure from breach, password managers have become a great alternative to remembering passwords or passphrases. They usually rely on a single master password you have to remember and then store all your passwords for any other account.

Resources

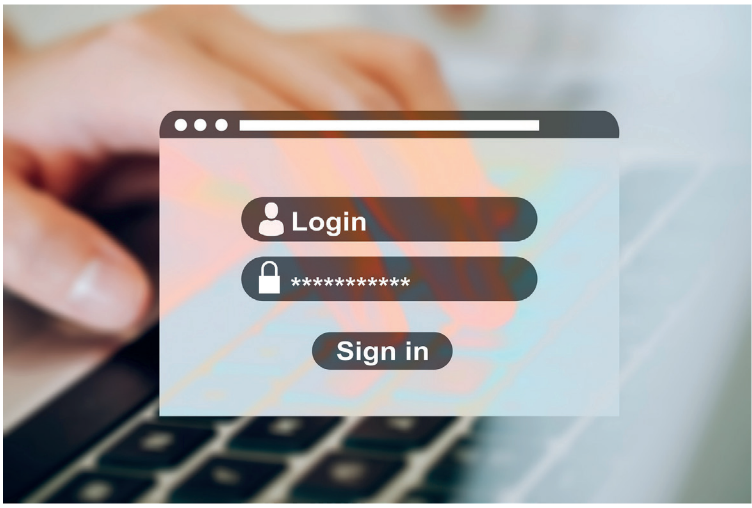
Dashlane

LastPass

KeePass

1Password

browser-based password managers.



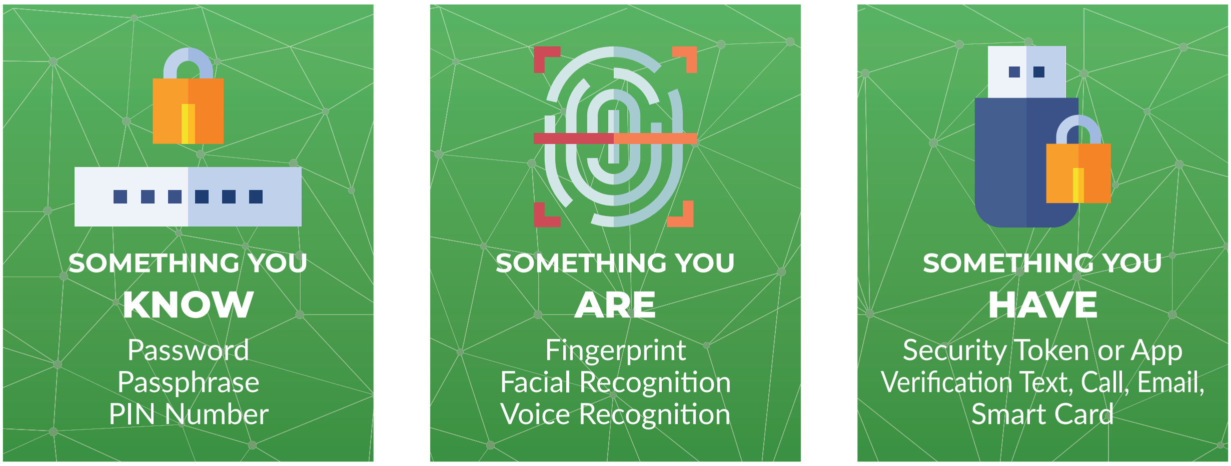
When you log in to a service, you use your master password to access the application-specific password. Password managers can also choose lengthy random complex passwords using a generator, so you never have to remember or even know all your passwords. Password managers also can identify when you are using an insecure password.

Multi-Factor Authentication

Further Strengthen your accounts using Multi-Factor Authentication (MFA)

As a designer, artist, or developer, you are likely going to have a public profile, which makes you a target for fraud as your contact information might appear in social media. Attackers will often try to use publicly available information to attempt brute-forcing attacks against victim login credentials to try and take control of those accounts. Multi-Factor Authentication (MFA) requires more than one authentication method from independent sources to verify your identity. In other words, you obtain the system access that you wish to use only after providing two or more pieces of information that uniquely identifies you.

There are three categories of credentials: something you either **know**, **have**, or **are**.



SOMETHING YOU
KNOW
Password
Passphrase
PIN Number

SOMETHING YOU
ARE
Fingerprint
Facial Recognition
Voice Recognition

SOMETHING YOU
HAVE
Security Token or App
Verification Text, Call, Email,
Smart Card

Figure 1 - Multi-Factor Authentication (MFA)

Many services offer multi-factor authentication (MFA). To help protect your accounts, check the settings with each service provider where you usually log in with a username and password. You can also contact the service provider's technical support to see if MFA is available. If MFA is available, enable it. This includes any account with a login such as emails, services portals, financial webpages, or desktop applications.

Resources

PCI-DSS MFA Guidance

NSA Guidance for MFA

List of Websites that offer MFA

Social Engineering

Think Before you Act!

Everyone can be victimized by social engineering, but as an artist you may be more at risk given the number of people you interact with, some of whom are known to you only in their virtual personas. Social engineering exploits our human nature, our desire to be helpful, or our submission to authority, and its practitioners craft realistic scenarios that lead you to believe they are someone you can trust before they exploit your trust for nefarious purposes. Cybercriminals have become quite savvy in their attempts to lure people in and get you to click on a link or open an attachment. If something seems unusual, practice caution. For example, if someone asks for you to perform a task via a virtual avatar or even through an SMS message that seems slightly out of character, follow up with a phone call or video conference. Given XR's potential to influence our reality, the threat of social engineering in the XR space requires mechanisms to validate identity and opens the door for sophisticated threat vectors, including the use of deep fakes.

If you are unsure whether an email request is legitimate, try to verify it with these steps:

- **Contact the sender directly**
  Using the information provided on any account statement, on the sender's official website or on the back of a credit card.

- **Search for the sender online**
  But not with the information provided in the email.

Resources

NCSA guidance on Spam and Phishing

Malware and Botnets

Protect yourself from unwanted, and potentially harmful, files or malicious programs

Malware and Viruses are harmful programs that can be transmitted to computers and other connected devices in several ways. Most commonly, viruses aim to give the criminals who create them some sort of access to the infected devices. Botnets are networks of computers infected by malware (such as computer viruses, keyloggers, and other malicious software) and controlled remotely by criminals, usually for financial gain or to launch attacks on websites or networks.

Install anti-malware and keep it up to date. Configure the anti-virus/anti-malware to scan regularly as well as in real-time. Keep your system up to date with the latest security updates.

Resources

Malware Protection Guidelines from US-CERT

SANS Institute Guidance for Malware Protection

MALWARE CLASSIFICATION

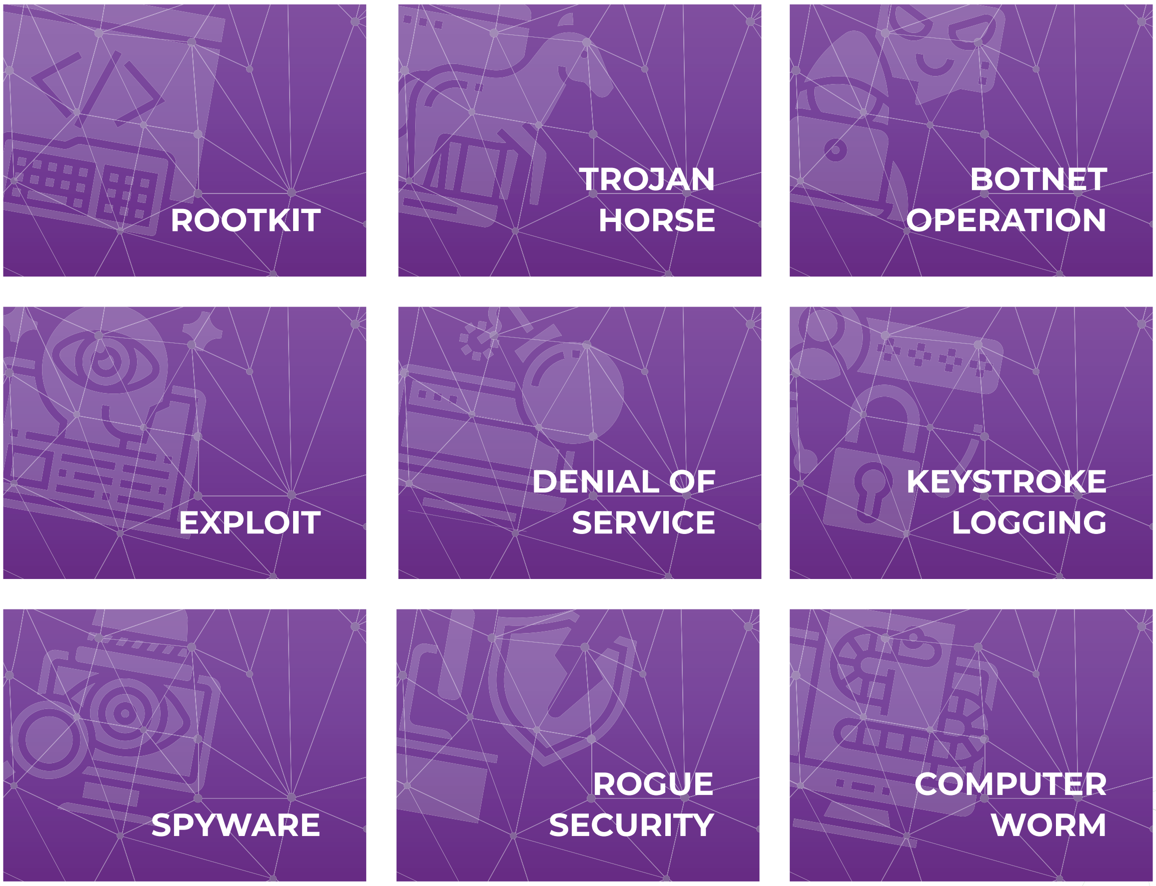


Figure 2. Malware Classification

Identity Management

Re-Examining Your Digital Footprint - Manage your identity to stay safe online

Identity management involves keeping track of what online accounts you have, on which platforms, and ensuring they are maintained. It is an often overlooked area as so many platforms require a login, and your identity is associated with several virtual selves. Your online identity includes aliases used across various platforms. Often your alias can be easily associated with your real identity through simple contact chaining. In many cases, an alias is intended to be a nickname, but if you want to protect your identity through it, you have to take special care to ensure your real name and your alias never appear together. It is essential to safeguard your online identities and maintain the personal information of each virtual self to help avoid data leak.

For any XR experiences involving individual identities, you should pay attention to the privacy policies and manage your online identity carefully via:

- Choosing how your name or alias appear to others in the experience;
- Deleting account history associated with the platform or experience;
- Editing your avatars or pictures associated with the platform or experience.

When it comes to XR, there is no anonymity, and there is currently no legal basis to prevent platform owners from constantly capturing your identity and associated data, including Biometric data. The best prevention is to be aware of this challenge and avoid the platforms that harvest data to further sell or monetize for profit.

Resources

How to remain Private in XR by Avi Bar-Zeev

Manage Privacy Settings to Stay Safe Online

Ransomware

Proactive defense is the best protection against Ransomware.

Ransomware is a family of malware that encrypts a user's files, and then the criminals behind it demand a fee to decrypt the files. It's commonly delivered via phishing emails but can originate from various sources, including sharing files with other artists.

Backups go a long way to protecting you from the impact of ransomware if you can effectively redeploy your experience and delete the compromised one.

However, if you do not have a recovery mechanism in place, you may be forced to negotiate with criminals or re-create your product from various previous unpolished versions. If you deal with user-generated content and curating content from other non-trusted sources, establish and maintain a mechanism to scan scripts and links for malicious code.

Resources

US Govt guidance on ransomware protection

Multi-stakeholder Ransomware Prevention advice

Update your Systems and Browsers

Protect your devices, systems, and software - keep them up to date!

To create artwork and build immersive experiences, you will often utilize third-party software and work with various vendor platforms and systems. When vendors become aware of vulnerabilities (weaknesses) in their products, they often issue patches to fix those vulnerabilities. Make sure to apply relevant patches to your computer as soon as possible so that your system is protected. Patching and staying up to date with the latest software versions is one of the most important aspects to avoid any breaches and data leaks.

Resources

Guidance on Patching and Updating

Following are some of the best practices to keep in mind for keeping your systems and software up to date:

- Enable automatic software updates whenever possible. This will ensure that software updates are installed as quickly as possible;
- Do not use unsupported EOL (End of Life) software;
- Always visit vendor sites directly rather than clicking on advertisements or email links;
- Avoid software updates while using untrusted networks.

New vulnerabilities are continually emerging, but the best defense against attackers exploiting patched vulnerabilities is simple: keep your software updated.

Intellectual Property

Exercise your Intellectual Property Rights!

In XR, how do you establish whose property/artwork is it, and who owns it?

Who owns what you create, depending on the tool you use? How does choosing a tool impacts who owns the art, and who can see it?

As an XR artist or developer, you must weigh-in several intellectual property considerations when creating new artwork. Even in novel XR technology landscapes, you must consider the possibility of lawsuits related to copyright, trademark, or right of publicity issues. As a creator, you should educate yourself and take these intellectual property implications into account. You should study these issues and consult a lawyer whenever unsure about something specific on intellectual property use. By cultivating critical thinking, consulting with a lawyer, and taking strong actions against Intellectual Property infringement, you can mitigate the risk of liability and focus your efforts on what matters most: creating the best XR artwork, platform, or experience.

While responding to Intellectual Property-related issues is mostly a reactive measure, some other areas must be addressed proactively.

For example:

1. The software and hardware used during the development of your creation must have all **valid licenses and ownership**;
2. You should consider relying upon and using **open source alternatives** when possible, Such as (WebXR Aframe) Open XR Standard;
3. **Provenance** - As indicated via the XRSI Privacy framework v1.0, you should maintain data provenance and lineage for review to ensure data integrity and ownership. There are integrity-checking tools currently being built in the XR domain that you should consider adopting and implementing. E.g., When you use a particular XR tool, does it mean the creation will be owned by the platform or organization who designed the tool or the creator, i.e., you?

Resources

Content Authenticity Initiative

The XR Safety Initiative

Top 4 Open Source AR tools

Aframe

WebXR

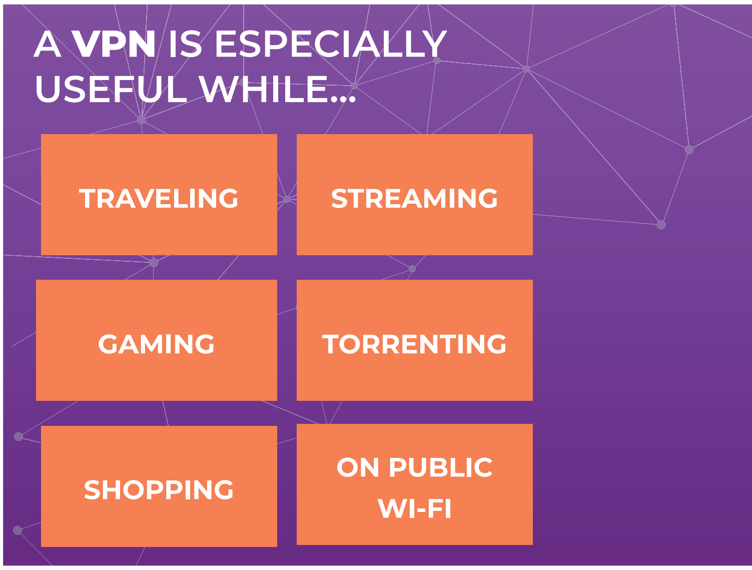
Virtual Private Network

Hide your location, protect privacy and enhance security via VPN

As an artist, privacy is important to you. You should use a Virtual Private Network (VPN) every time you connect to the internet. A VPN is a secure tunnel between your device and the Internet, protecting your online traffic from snooping, interference, and censorship. A VPN app runs in the background of your device, so it won't get in the way while you use other apps, stream content, and browse the internet.

Alternatives to VPN

A VPN isn't the only tool to increase your privacy, security, and freedom online. There is Tor—aka Onion browser—and Proxy services. However, a trustworthy VPN is still the best privacy solution for most people.



A **VPN** IS ESPECIALLY USEFUL WHILE...

TRAVELING

STREAMING

GAMING

TORRENTING

SHOPPING

ON PUBLIC WI-FI

Figure 3. Situations in which a VPN is especially useful

Resources

NordVPN

ExpressVPN

Surfshark

CyberGhost

Private Internet Access

Maintain Backups

Prepare for the worst!

Data can be lost in several incidents, including computer malfunctions, theft, viruses, spyware, accidental deletion, and natural disasters.
So it makes sense to back up your files regularly.

A data backup is a simple, three-step process:

- **Make copies of your data;**
- **Select the hardware or method to store your data;**
- **Safely store the backup device that holds your copied files (for local backups).**

Resources

Apple
Backup your Mac
Time Machine
iCloud for Apple iOs devices

Windows
Windows 10
Windows 7
Windows Vista and older

One of the best ways to keep your experience available is to have backups ready in case of a destructive incident. Depending on where you host your experience, your service provider might already have backup functionality available. For example, if you host infrastructure in AWS or Azure cloud computing platforms, you can purchase redundancy and backup as a service. Aside from that, even just writing your work to an external hard drive can help. However, relying on your service provider to provide backups can save you time when a recovery is needed. Whatever service providers you work with, be sure to talk to them about backup and recovery.

CHAPTER 2

ADVANCED **PRIVACY AND SECURITY** ENHANCING TIPS

XR Individual Artists, Creative collaborators, Artistic developers, and XR Program Managers can use these advanced tips to further enhance the privacy and security for a particular project or team.

*In an era when
“Seeing is no longer believing,”
we must focus on building
trust and human safety.*

-Kavya Pearlman, CEO - XRSI

Trust and Safety in the XR Domain

The primary consumers of the XR domain are humans, and therefore awareness becomes a key component of minimizing risk. In the immersive technology domain, we often dance around various terms to refer to the unintended consequences associated with the use of these technologies. While some call an aspect of an ethical dilemma, others refer to them as “security and privacy challenges,” and sometimes all the issues are lumped into “ethical concerns.”Once we start to zoom out, what we discover is it is all about ensuring safety and, as a result, achieving trust.

XR technologies empower us to enjoy experiences and applications never before possible by collecting precise data about the environment and how an individual interacts with it, using sensors and on-device tracking mechanisms. However, the most significant challenge lies in addressing how data is collected, processed, stored, and destroyed safely and ethically.

Given the scope and complexity of data processed and potentially collected in XR, special care must be taken to ensure you respect the privacy of individuals, including bystanders. Some of the data transmitted from XR devices can be classified as biometric Inferred Data and should only be stored for well-defined purposes. The more you understand about the kinds of data you collect and who you are sharing the data with, the better prepared you’ll be to ensure you adhere to existing and future privacy laws such as General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA).

Always collect the least amount of data you need to achieve your goal. For many experiences, you might not have to collect data at all, but rather process and forget. If you choose to collect data, be sure that you've provided individuals with a privacy policy that outlines what you collect and how you use that data. There are some publicly available tools to help you craft a privacy policy and even terms of service.

You must take the time to understand what you are collecting. If you aren't heavily involved with the actual development of the experience, speak with your developers, and have a discussion about what data is collected from each individual and whether it's strictly necessary. In most cases, less is better.

If you collect data, protect it. Ensure your platforms encrypt all data in-transit and at rest. Once an individual has agreed to provide you data, you should make every reasonable effort to keep it safe. In every case, establish a mechanism to acquire consent from individuals. This is important to inform individuals of your intent, but will also help protect you later.

You should take special care if you are designing an experience for minors. While the definition of "minor" may vary from jurisdiction, most jurisdictions have guidelines for how you can process, collect, and share data for individuals under 18.

Make Future Truly Private with the XRSI Privacy Framework v 1.0

Launched in September 2020, The XRSI Privacy Framework version 1.0 offers a toolkit to empower artists, individuals, and organizations with a common language and a collection of safety and privacy controls to address diverse privacy and security needs. This framework draws a baseline of solution-based controls with principles like "privacy by design" and "privacy by default" baked in, driven by trust, transparency, accountability, and human-centric design.

The Privacy Framework comprises three layers:

- **Focus Areas**
- **Set of Functions**
- **granular controls**

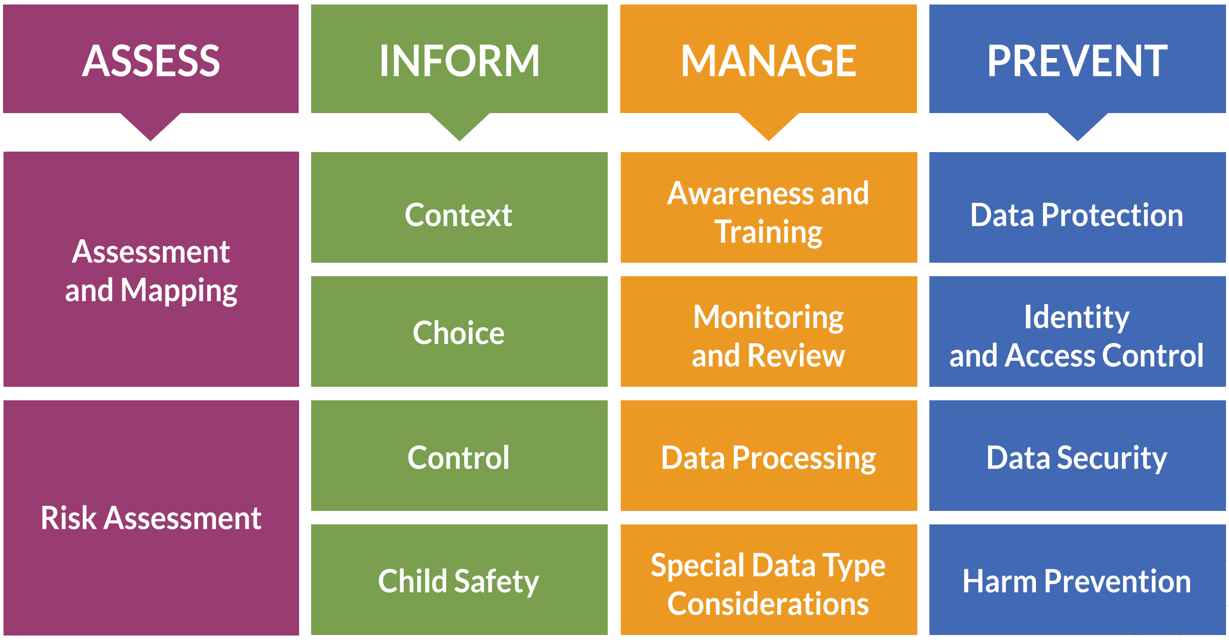
Each component reinforces how you can achieve privacy goals through aligning strategies, responsibilities, and activities to prevent harm to humans in XR environments.

Resources

The XRSI Privacy framework v1.0

Immersive Standards for Accessibility Ethics, Inclusion and Safety 1.0

Code of Conduct - XRSI



ASSESS	INFORM	MANAGE	PREVENT
Assessment and Mapping	Context	Awareness and Training	Data Protection
	Choice	Monitoring and Review	Identity and Access Control
Risk Assessment	Control	Data Processing	Data Security
	Child Safety	Special Data Type Considerations	Harm Prevention

Figure 4 - Areas of Work and Subcategories in the XRSI privacy Framework

Focus Areas Overview

#1 ASSESS

By nature, XR applications are multi-modal and often use the full suite of sensors available on a given XR-enabled device. For instance, AR frameworks often use data from a mobile device's camera, combined with the data from the gyroscope and the acceleration sensor to determine the device's position in space.

Each data set a company collects comes with complications. First, it's essential to assess what data is required to facilitate the experience and then evaluate what data needs to be stored. Thereafter, you need to conduct a risk assessment to determine the impact on the project operations, mission, and functions while considering other risk factors, including human, societal, informational, financial, and legal areas.

A Framework for XR Risk Assessment

Human	Societal	Information	Financial	Legal
Physical harm *Motion Sickness* *Hygiene* *Physical Injury*	Manipulated Social Discourse *Disinformation* *Propaganda* *Misinformation* *Deep Fakes* *Deep Nudes* *Discrimination*	Lack of Standardization *Unintended Information Disclosure*	Denial of Service	Harm caused by Robotic interfaces
Psychological Harm *Loss of Trust* *Cognitive Dissonance* *Addiction and dependency* *Virtual Embodiment/ Body Dysmorphia* *Body Swapping* *Superrealism - "This is where awareness becomes crucial"* *Phantom Timeline Syndrome*	Spectator Culture	Identity Theft	Data Breach	Exploiting Loss or Trauma
Unethical Behavior *Bullying* *HarassmentViolence* *Abuse* *Stalking*	Child Safety	Misuse of data	Payment and Transaction Integrity	Lack of Consent
Content-Induced Risks	Digital Divide / Device Gap	Third-party risks	Blackmail / Ransomware	Persuasion to cause criminal behavior
Child Safety	Societal Trust / Lack of Ground Truth	Cybersecurity *Social Engineering* *Novel cyberattacks in XR* *Application Vulnerabilities* *Malware / Virus*	Account TakeOver	Intellectual Property
Defamation	User Generated Contents *Malware Injection*	Privacy Violations *Excessive data collection* *Misuse of data* *Data Loss*	Pick Pockets	Provenance
		XR Device Tampering	Fraud	Inability to establish Truth
			Gambling	Compliance with Regulations
			Money Laundering	
			Microtransactions - aggressive pay to win	
			Fictitious sales/ discounts	

Figure 5 - A framework for XR risk assessment

#2 INFORM

Informing individuals about privacy risks begins by first understanding their privacy needs and expectations. Privacy needs can be derived from individuals' legal privacy rights, whereas the context and choice are communicated in the form of privacy policy based on the overall understanding of privacy expectations. Privacy disclosures are essential to XR, providing insight and transparency into what information is being collected by XR devices and how this information is being used. Legally-mandated "privacy policies" are not sufficient to inform individuals about (1) how do you affirmatively protect privacy and (2) how do you use (or may use at a later stage) personal and sensitive XR data, including biometrically-inferred data. Therefore, communicate clearly, transparently, and effectively to empower individuals in making informed decisions about how their data is processed as well as what kind of risks may be associated with such data processing.

Resources

The XRSI Privacy framework v1.0

Immersive Standards for Accessibility Ethics, Inclusion and Safety 1.0

Code of Conduct - XRSI

#3 MANAGE

You should manage privacy risk by establishing mitigating controls such as reasonable data security protections; taking into account the costs of available security controls and tools; the sophistication and size of the project in scope; and sensitivity of the associated personal and XR data. You should establish project priorities, constraints, risk tolerance, and assumptions and use those to support risk decisions associated with managing privacy risk and third parties within the data processing ecosystem. You should establish and implement the processes to identify, assess, manage, and protect individuals' privacy, increase manageability, and implement privacy principles (e.g., individual participation, data quality, and data minimization).

#4 PREVENT

Be Proactive not Reactive. Be Preventative not Remedial. Anticipate and prevent privacy incidents before they happen, to protect yourself and your audience from privacy issues that could potentially hurt your reputation. Maintain security and privacy policies (e.g., purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment), processes, and procedures and use them to prevent harm. One such proactive measure is safety and privacy by design. The need for such an approach is becoming more evident every day. It is all about enabling trust in systems, designs, and data so that organizations can lead to transformational change and innovate with confidence.

Be Safe,
Be Private,
and Build a
Culture of Care,
Inclusion,
and Awareness!

XRSI

CYBER-XR COALITION

ARTIZEN

RH1
READY HACKER 1

Emerging technologies are typically software, systems, and platforms developing at a rapid pace. So, creatives and developers are called to move fast to be one step ahead of the rest of the world, to anticipate the transformations, and set trends. Such a competition, where time is a crucial factor, needs to be associated with the "culture of care."

The catalyzing event of COVID-19 has highlighted and underscored the importance of emerging realities to bring people closer and create a virtual society that is inclusive and aware. The artists' community holds the power to shape our cultures and societies while reducing the unintended consequences and minimizing risks. The artists and developers should remain aware of the risks associated with their creations and take steps to prevent or counteract the negative impacts.

Resources

Immersive Standards for Accessibility Ethics, Inclusion and Safety 1.0

Code of Conduct - XRSI

During the whole project development cycle from ideation to execution, you should include a diverse group to ensure that your project is accessible, has a broader outreach, and contributes to creating and maintaining a sustainable future for the XR ecosystem. When creating immersive content, you should make every effort to warn Individuals of situations when it is unsafe to engage with your experience.

The "culture of care" is a complex set of values and actions, spanning from respect for standards and regulations to minimizing risks and preventing harm. It requires deliberate effort to put processes in place that promote a sense of care for humanity and broad awareness of the impact these systems and platforms have on humans. This culture should arise from due diligence and internal integrity to ensure the end products are accessible and that they do not compromise on trust and safety or take away from it the factors of inclusion.

When in doubt about the ethical foundation for extending realities, you can lean on the Cyber XR Coalition Goals outlined within **Immersive Standards for Accessibility Ethics, Inclusion, and Safety 1.0**, which are:

1. **Leave no one behind**
2. **Be accessible**
   Everyone must be able to participate in the digital society
3. **Protect identities**
   Individuals must be able to participate in the digital society no matter their gender, ethnicity, birthplace, or cultural and political beliefs, ensuring discrimination and biases are mitigated and not further reinforced
4. **Keep everyone safe and secure**
   Shape rules and practices to enable a secure and resilient immersive environment
5. **Build new rules to promote trust**
   Develop new, flexible, participatory governance mechanisms to complement traditional policy and regulation in a domain that's in constant evolution

XRSI CYBER-XR COALITION ARTIZEN RH1 READY HACKER 1