

## DATA &amp; PRIVACY TRANSPARENCY REPORT

# Overview of ZeroEyes Data Retention and Privacy Practices

**Recognize the object.**  
**Verify the object.**  
**Communicate the information.**

ZeroEyes exists to shorten the time between a firearm or bladed object appearing and a first responder knowing about it. That mission does not require us to identify a person by name, or continuously track a person. It requires us to recognize an object, verify that object, and communicate that information to our clients as fast as possible.

## WHAT ZEROEYES NEEDS TO KNOW

The object. Enough to recognize it, verify it, and communicate it to the client.

## WHAT ZEROEYES DOES NOT NEED

A person's name or to continuously track a person.

## SCOPE

This Standard governs the ZeroEyes AI threat detection platform and the ZeroEyes Operations Center in all deployments.

Public sector organizations

Private sector organizations

## WHAT IT APPLIES TO

Imagery and metadata that we process or review (by a real person).



## Customer camera systems remain under customer control.

The customer uses ZeroEyes software in connection with its own video management system, which remains entirely under customer control and authority.

# What ZeroEyes Detects — and What It Does Not

## WHAT THE SYSTEM DETECTS

ZeroEyes analyzes frames from cameras customers already own and operate to identify:

### Visible, brandished firearms or bladed objects

Detection is focused on the object — not on identifying the person carrying it.

Cameras remain the customer's own. ZeroEyes reads frames from them; it does not add cameras, move them, or watch a continuous live feed.

## WHAT THE SYSTEM DOES NOT DO

ZeroEyes does not perform, and is not built to perform:

- ✗ Facial recognition or face matching
- ✗ Identity resolution against any database, government or commercial
- ✗ License plate reading or vehicle tracking
- ✗ Gait analysis
- ✗ Biometric analysis
- ✗ Emotion or affect analysis
- ✗ Behavioral profiling
- ✗ Threat scoring
- ✗ Anomaly detection on people
- ✗ Attendance monitoring
- ✗ Productivity monitoring
- ✗ Conduct monitoring
- ✗ Audio capture or analysis
- ✗ Predictive analysis

"Privacy is an important part of this rollout. ZeroEyes is designed to identify only visibly brandished weapons – not individuals. Operations Center screens remain blank unless a potential weapon is detected, and team members do not watch a continuous live camera feed. The platform does not perform facial recognition and does not store personal or biometric data."

**THORNTON TOWNSHIP HIGH SCHOOL DISTRICT 205**

### A detection event creates a bounded data record.

-  Key-frame image containing the detected weapon
-  Corresponding camera image frame
-  Camera geographic coordinates
-  Camera identifier
-  Unique alert identifier

## ZeroEyes only captures images.

ZeroEyes does not append third-party data to an image capture for the purpose of identifying a person. ZeroEyes does not control how its customers use the images, or their identification of any person.

## DATA RETENTION

| DATA TYPE                                                                                                                                                       | RETENTION                                                     | DELETION  |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|-----------|
| Verified true-positive detection imagery                                                                                                                        | Retained indefinitely                                         | Manual    |
| Analyst-dismissed / false-positive imagery                                                                                                                      | Discarded within 30 days                                      | Automatic |
| Detection metadata and audit logs                                                                                                                               | Retained indefinitely                                         | Manual    |
| Imagery under active legal hold                                                                                                                                 | Retained indefinitely; deleted upon release of the legal hold | Manual    |
| Customers may request a shorter retention window than our default, and may request certified deletion of all imagery associated with their account at any time. |                                                               |           |

# Customer Ownership, Access and Data Sharing

**Your cameras.**  
**Your imagery.**  
**Your data.**

All imagery originating from a customer's cameras remains the customer's property. ZeroEyes claims no ownership interest in customer imagery.

ZeroEyes obtains a license to the data only to provide the service:

Detecting potential weapons

Transmitting a detection frame

Presenting it to a verifying analyst

Dispatching an alert

The license terminates on contract termination, at which point associated imagery is deleted and deletion is certified — unless otherwise required by law or requested by the customer.

## NO CROSS-CUSTOMER SURVEILLANCE NETWORK



### No cross-customer network

ZeroEyes does not use information from one customer for the purpose of providing service to a different customer.



### No third-party query interface

No outside agency can search ZeroEyes data.



### No commercial data sales

ZeroEyes does not sell, rent, or license customer imagery or detection data to data brokers, advertisers, or insurers for their own use.



### Customer-controlled alert distribution

Customers control who will receive the alerts, and may change that distribution list at any time.

## SUBPROCESSORS



ZeroEyes provides a list of subprocessors on request and as required by law.

# Human Verification at the Center

## AI detects. A trained human verifies.

No alert reaches a first responder without review and confirmation by a trained ZeroEyes analyst.

### THE SYSTEM DOES NOT INDEPENDENTLY

- ✗ Lock doors
- ✗ Notify police
- ✗ Dispatch responders
- ✗ Escalate an incident

### Verification Standard



The ZOC is designed to verify clear, actionable detections with speed, while allowing additional time for review when a situation is ambiguous.

## ZEROEYES OPERATIONS CENTER — HOW ANALYSTS ARE TRAINED AND SUPPORTED

### 01 Initial training and evaluation

New Analysts complete structured onboarding and a probationary evaluation period prior to assuming independent duties.

### 02 Supervised monitoring

New Analysts monitor under the direct oversight of experienced personnel and are assigned independent responsibilities only upon demonstrated readiness.

### 03 Team-based operations

The ZOC operates on a 24/7 basis, with peer, senior, and management support available for escalation or supervisory review.

### 04 Contextual Decision-Making

Analysts evaluate each detection against available situational context and escalate whenever a determination is not clear-cut.

### 05 Ongoing training and evaluation

Analysts are assessed on a recurring cycle and receive continuing training and coaching throughout their tenure.

### 06 Professional development

Analysts pursue relevant external certifications in emergency communications and security in support of their continued development.

## ACCOUNTABILITY AND RESTRICTED ACCESS



### Logging

All analyst actions are logged and attributable; logs are maintained for auditability and quality assurance.



### Access Restriction

Analysts are restricted to viewing the specific detection under review and do not have access to live feeds or unrelated footage.



### Statement of Understanding

All Analysts operate under a duty of confidentiality where required by applicable law.

# Transparency, Customer Control and Clear Limits

## AUDITABILITY AND CUSTOMER CONTROL

Customers receive upon request:

- ✓ Access to maintained audit logs of detections, analyst dispositions, and alert dispatches for their own sites
- ✓ An annual account-level summary: detection volume, verification outcomes, and alert dispatches

## LEGAL PROCESS

ZeroEyes will disclose customer data where required by law, or where it believes doing so is necessary or appropriate, as permitted by applicable law and contract.

ZeroEyes will also maintain data where required by law, or where it believes it is necessary to do so.

## Accuracy, limits, and what this technology cannot do

EXPOSED WEAPONS ONLY

### Visible weapons only

The system detects visible weapons only. It cannot detect a weapon concealed in clothing, a bag, or a vehicle, and it is not a substitute for a screening or entry-control layer.

### Camera coverage matters

Camera coverage is the binding constraint. A firearm outside a camera's field of view, obscured, or in poor lighting will not be detected. Detection performance is a function of the customer's existing camera placement, resolution, and lighting.

### False positives can occur

Human verification exists to mitigate a false detection becoming a dispatch. ZeroEyes attempts to de-escalate a response with highly trained analysts, and errs on the side of caution.

### ZeroEyes does not claim to prevent shootings

ZeroEyes claims to reduce the time between a firearm or blade becoming visible and a responder having actionable information about it. No published research establishes that camera-based AI detection prevents attacks, and we will not imply otherwise.

### ZeroEyes is one layer of security

Detection without a rehearsed response protocol produces confusion, not safety. ZeroEyes provides a white-glove onboarding service to help clients weave ZeroEyes detections into their broader active assailant response protocols.

## Threat detection does not require **identity surveillance**.

ZeroEyes is designed to recognize visible threat objects, add trained human verification, and deliver actionable information — while maintaining clear boundaries around privacy, access, and customer control.