PRIVACY & MISUSE RISK CONTROLS

Plain-Language Risk and Control Summary

A leadership and stakeholder reference for understanding key privacy and misuse risks associated with license plate reader (LPR) technology.

Purpose

This document explains key privacy and misuse risks related to the use of license plate reader (LPR) technology and the controls used to reduce those risks.

The goal is to answer three simple questions for each risk:

1. What could go wrong?
2. What controls do we need to reduce the risk?
3. Why are those controls important?

Controls do not mean that a risk can never happen. They provide safeguards that help prevent problems, find problems when they occur, and make sure appropriate action is taken.

Risk 9 — Cameras Collect Information They Should Not Collect

What could go wrong?

A camera could collect information outside of what the program is allowed or intended to collect. This could create privacy concerns and cause the system to collect more information than is needed.

Controls we need

Camera Setup and Configuration Checks

Make sure each camera is set up to collect only the information it is supposed to collect.

Privacy Review Before Installation

Before a camera is installed in a new location, review how it will be used and whether it could collect information it should not.

Testing After Changes

When cameras, software, or settings are changed, test them to make sure privacy protections still work as expected.

Why this is important

People expect the system to collect only the information needed for its approved purpose. These controls help prevent the collection of unnecessary information and reduce privacy risk.

Risk 11 — Someone Who Should Not Have Access Gets Into the System

What could go wrong?

A person who does not need access could see or search license plate information.

This could happen because access was given to the wrong person, an employee changed jobs but kept access, or someone's password was compromised.

Controls we need

Role-Based Access

Only give people access to the information and system functions they need to do their jobs.

Regular User Access Reviews

Review the list of users regularly. Remove access when someone leaves, changes jobs, or no longer needs the system.

Extra Login Protection
Require an additional security step when users sign in so that a password alone is not enough to access the system.

Why this is important
License plate information should only be available to people who have an approved need to use it. These controls help keep unauthorized people out of the system and limit what authorized users can access.

Risk 12 — Different Agencies Follow Different Access Rules

What could go wrong?

When several agencies use or share the same information, one agency could have stronger protections than another.

This could create a weak point in the overall program.

Controls we need

Common Access Standards
Establish basic access and security rules that every participating agency must follow.

Written Agreements
Clearly document what each participating agency is allowed to do with the information and what security and privacy requirements it must follow.

Cross-Agency Reviews
Periodically verify that participating agencies continue to follow the agreed-upon rules.

Why this is important
Information should receive appropriate protection regardless of which participating agency is using it. Shared information also creates shared responsibility.

Risk 14 — Someone Searches License Plate Information Without a Proper Reason

What could go wrong?

Someone with access to the system could search for a person or vehicle without an approved reason.

For example, a user could search because they are curious rather than because the search is connected to an approved purpose.

Controls we need

Require a Reason for Every Search
Users must provide an approved reason before conducting a search.

Record Search Activity
Keep a record showing who performed the search, when it occurred, and other information needed to review the activity.

Review Search Activity
Regularly review searches to make sure users are following the rules.

User Training
Teach users what is and is not an appropriate reason to use the system.

Why this is important
Having access to a system does not mean someone should be able to search for anyone they want. These controls help make sure the system is used for an approved purpose and provide a record that can be reviewed if questions arise.

Risk 15 — An Authorized User Misuses the System

What could go wrong?

A person may have legitimate access to the system but still use it in a way that is not allowed.

Because the person is an authorized user, simply controlling who can log in is not enough.

Controls we need

Monitor for Unusual Activity
Look for searches or patterns of activity that may be unusual or inconsistent with normal use.

Investigate Alerts
When unusual activity is identified, review it to determine whether the activity was appropriate.

Clear Misuse Rules
Have written policies explaining acceptable use and what happens when someone violates those rules.

Document Investigations and Actions
Keep records showing how suspected misuse was reviewed and what action was taken.

Why this is important
Access controls help determine who can get into the system. Monitoring helps determine what people do after they get in. Both are needed to protect information from misuse.

Risk 19 — Information Is Kept Longer Than It Should Be

What could go wrong?

License plate information could remain in the system after the approved retention period has ended.

Over time, this could result in the organization keeping much more information than it needs.

Controls we need

Clear Retention Rules
Define how long information should be kept.

Automatic Deletion
When possible, configure the system to automatically delete information after the approved retention period.

Retention Reviews
Regularly check that information that should have been deleted is no longer being stored.

Legal Hold Process
If information must be kept longer because it is needed for an investigation, court case, or another approved legal reason, clearly identify and protect that information.

Why this is important
Information should not be kept forever simply because it was collected. Keeping information only as long as needed reduces privacy and security risk while still allowing information to be preserved when there is a legitimate reason to keep it.

Risk 21 — Misuse Happens, but the Audit Process Does Not Catch It

What could go wrong?

Someone could misuse the system, but the organization might not discover it if activity is not properly recorded and reviewed.

Controls we need

Keep Audit Records
Record important system and user activity.

Regularly Review Activity
Review audit information for unusual or inappropriate activity.

Include All Appropriate Users and Agencies
Make sure monitoring covers the people and organizations that have access to the system.

Track Problems Until They Are Resolved
When a potential issue is identified, document it and follow it through investigation and resolution.

Why this is important
A rule is much harder to enforce if there is no way to tell whether someone followed it. Audit records provide accountability and help the organization identify, investigate, and correct possible misuse.

Risk 22 — Someone Changes or Deletes the Audit Records

What could go wrong?

If users can change or delete audit records, someone could misuse the system and then try to hide what they did.

Missing or unreliable records could also make it difficult to investigate an incident.

Controls we need

Protect Audit Logs
Limit who can change, delete, or manage audit records.

Check for Missing Records
Use processes or technology to identify unexpected gaps in audit information.

Investigate Missing or Unusual Information
Review unexplained gaps or changes to determine what happened.

Protect Audit Records for the Required Period

Keep audit information long enough to support reviews, investigations, and other requirements.

Why this is important

The audit trail tells us what happened in the system. If that record cannot be trusted, it becomes much harder to identify misuse or hold people accountable.

How These Controls Work Together

No single control can address every privacy or misuse risk. Instead, the controls work together in layers:

We want to make sure…	Controls help us…
We collect only what we need	Review camera placement, settings, and privacy impacts
Only the right people have access	Control access and regularly review users
People use the system for the right reasons	Require a reason for searches and train users
We can identify possible misuse	Record and review user activity
Misuse has consequences	Investigate problems and follow established policies
We do not keep information forever	Apply retention and deletion rules
We can trust our records	Protect audit logs from changes or deletion

Key Takeaway

The purpose of these controls is not simply to have more rules.

Together, they help answer important questions:

- Are we collecting only what we need?
- Are only the right people using the system?
- Are they using it for an approved reason?
- Can we tell if someone misuses it?
- Do we take action when something goes wrong?
- Are we deleting information when we no longer need it?

Why this is important

When the answer to those questions can be supported with evidence, the organization is in a much stronger position to show that privacy and misuse risks are being actively managed.