2026 Privacy Impact Assessment

LiveView Technologies (LVT for FAS)

FAS

Seattle Information Technology

Contents

Privacy Impact Assessment overview.....2

1.0 Overview 3

2.0 Data Details & Collection Practices 4

3.0 Data Use & Processing 5

4.0 Legal Scope & Compliance 7

5.0 Data Security, Protection, & Storage.....8

6.0 Data Sharing & Disclosure 9

7.0 Data Retention & Destruction.....11

8.0 Privacy Principles, Risks, & Controls.....12

Seattle Information Technology

Privacy Impact Assessment Overview

What is a Privacy Impact Assessment?

A Privacy Impact Assessment ("PIA") is an analysis of how personal data is gathered, processed, and used for a particular program, project, data initiative, or technology implementation (the terms may collectively be referred to hereafter as "effort"). The PIA asks questions about the collection, use, sharing, security and access of data involved in a City department effort. It also requests information about policies, training and documentation that govern use of the data and any associated technology. The PIA responses are used to determine privacy risks and mitigation measures to reduce those risks. To ensure transparency about personal data collection and management, the City of Seattle has committed to publishing all PIAs on an outward facing website for public access.

When is a PIA required?

A PIA may be required when a project, program, or other data processing activity has been flagged through the privacy review process as having a high privacy risk.

How to complete this document?

As department staff complete the document, they should keep the following in mind.

- Department Subject Matter Experts (SME) are responsible for providing responses to the questions. *Please do not edit the questions or question descriptions that are part of the template.*
- All content in this report will eventually be published to the public. Therefore, avoid using acronyms, slang, or other terms which may not be well-known to external audiences. Additionally, responses should be written principally using non-technical language to ensure they are understood by audiences unfamiliar with the topic.

Seattle Information Technology

1.0 Overview

1.1 Description: Please describe the effort.

Live View Technologies (LVT) provide advanced mobile and cloud-based solutions designed to enhance safety and security across various industries. These technologies integrate intelligent security features like real-time alerts and multi-system compatibility into user-friendly platforms.

Security cameras: FAS is trying to assist other departments in getting trailer style security cameras on FAS property for security purposes.

This PIA covers FAS use of the security cameras at the listed locations only.

Any other LVT systems will require a privacy assessment prior to purchase.

These would be locations that primarily yards, or infrastructure storage so are not accessible to the public (rarely).

The aim is to prevent vandalism, theft etc of City assets.

The following services of LVT will be provided:

LVT will be providing a Platform-as-a-Service (SaaS) Cloud solution for remote video and analytic data gathering, processing, Video Management System (VMS) – View live video stream, utilize panoramic, tilt, and zoom to position the camera perspective, pull archived video footage. Command Center if applicable – event alert monitoring. When a certain activity is detected, an event is triggered for review by employees or third-party monitoring. Limited AI-Based Video Analytics (described in depth below) is utilized on Security Unit cameras to identify objects of interest for the purpose of notifying and alerting security operators of a potential intrusion.

The analytics engine is entirely localized on the camera's computational unit.

Joint Training Facility
Charles St Yard
Haller Lake Yard
Sunny Jim Yard
Airport Way Center
Rainier Warehouse

1.2 Business Need: What business need/problem does this effort address?

Security cameras for specific FAS sites as deterrent as well as supporting FAS blanket contract for this technology.

FAS is trying to assist other departments in getting trailer style security cameras on FAS property for security purposes.

While FAS will handle a blanket contract for this, each department wanting to procure/use system will need to go through ask for new technology AFNT to assess whether this is Surveillance (use case based).

1.3 Benefits: What are the anticipated benefits of this effort and how does it relate to departmental and/or City mission?

This system acts as a deterrent and also if event occurs, can be used for evidentiary purposes.

1.4 Technology Details: Describe all technologies that support or will be used as part of the effort.

LVT will be providing a Platform-as-a-Service (SaaS) Cloud solution for remote video and analytic data gathering, processing, Video Management System (VMS) – View live video stream, utilize panoramic, tilt, and zoom to position the camera perspective, pull archived video footage. Command Center if applicable – event alert monitoring. When a certain activity is detected, an event is triggered for review by employees or third-party monitoring.

Limited AI-Based Video Analytics is utilized on Security Unit cameras to identify objects of interest for the purpose of notifying and alerting security operators of a potential intrusion. The analytics engine is entirely localized on the camera's computational unit.

1.5 Scope of Involvement & Use: Who is involved in the implementation or use of the technology, project, and associated data?

FAS will be responsible for managing the contract. At the specified locations, FAS will be responsible for the use of the system.

Where will the data be stored?
LVT will be responsible for hosting the technology.

2.0 Data Details & Collection Practices

2.1 Data Subjects: Whose data will be collected or processed as part of this effort?

Data subject may include, but are not limited to, City of Seattle staff and/or folks on site at the specified locations. The security cameras are facing spaces that are not in public spaces.

2.2 Data Fields: What are the data fields and data types that are involved in this effort?

Footage of site is collected. Incidental footage of staff or folks trespassing may be captured but signs will be posted that there are security cameras onsite. Any footage that is captured will be stored for specified time period.

2.3 Data Collection: How is the data collected for this effort? What are the data sources for the data used or processed as part of this effort?

LVT offers two trailer models with fixed head-mount units, designed to meet diverse customer needs. Seattle won't be "purchasing" anything but subscribing to the specified units. Cameras will be facing specified areas and will be clearly marked. These are not mounted in areas where there is foot traffic and footage is directly collected from an individual due to filming. These will remain in the areas specified and will not be moved without notice and updated information to the assessment and PIA.

2.4 Data Flow: Describe how data collected flows through the data lifecycle including the assets used to store and process the data. ("Assets" are things that support the information-related activities, such as software systems, appliances, databases, etc.)

Data is collected by the Live Unit, where it is initially stored for approximately 30 days. As the storage fills, older footage is overwritten by new footage. Any footage requested by a user is uploaded to the cloud environment hosted within AWS. Data remains on the mobile security unit until the unit is moved or as required by law, after which it is securely deleted.

In accordance with the City AI contract language, there will be no training on City of Seattle data.

2.5 Notice: At the point of data collection, how are individuals notified about the City's use, sharing, and disclosure of their personal data?

Yes. The facilities are not generally open to the public. However, signs will be posted as well as a motion activated spoken-alert warning that will notify folks that they will be recorded.

3.0 Data Use & Processing

3.1 Authorized Data Uses: What are the authorized uses of the data associated with this effort?

System will be recording and retaining data for 30 days. Recordings will be hosted on LVT cloud.

Captured footage of an incident may include information related to vandalism, theft and may include personal information as well (such as clothing, height, etc).

This information will be collected to understand what happened during the incident.

3.2 Authorized Technology Uses: What are the authorized use cases for the technology associated with this effort? How may the technology be used?

The technology will be used as a security camera at the listed sites.
**ALPR functionality with the product/service: ** is disabled and WILL NOT BE USED.
**Facial recognition or facial detection capabilities with the product/service is disabled and WILL NOT BE USED.
AI/ML types being used? Object detection. LVT utilizes ML models at the edge (Camera), and they do not have any of the advanced forensic features like "Gender, color, vehicle type, etc., they can only differentiate broadly between a human and a vehicle.

3.3 Use & Management Policies: What policies (City or department-specific) apply to the use and management of the data *and* technology (if different than the data) associated with this effort?

All personnel using the LVT system under Finance and Administrative Services (FAS) are required to adhere to strict policies and undergo relevant training to ensure the ethical, secure, and compliant use of this technology.

LVT applicable policies:
Information Security Policy
Risk Management Policy
Data Classification Policy

Data Protection & Retention Policy
Customer Data Access Policy
Acceptable Use Policy
Asset Management Policy
Network Security Policy
Identity and Access Control Policy
Incident Response Plan
Logging and Monitoring Policy
Change Management Policy
Vendor Management Policy
Backup Policy
Disaster Recovery Plan

**All LVT redacted policies are available at our Trust Center @ https://trust.lvt.com/.

3.4 Data Processing & Analytics: Please describe how the data will be processed and analyzed in support of the intended business goal/outcome. Please include metrics.

Data collected by the system is processed to support defined security, safety, and operational objectives. Video streams are analyzed using automated video analytics to detect predefined events such as intrusion, presence in restricted areas, loitering, or safety zone violations. Processing is primarily event-based and does not involve continuous human monitoring.

When an event is detected, the system generates metadata including event type, timestamp, device or camera identifier, and location or zone identifier. This metadata is used to trigger alerts, support incident response, and enable post-event review. Video review by authorized users occurs only in response to alerts or during investigations.

Analytics focus on aggregating event metadata to identify trends, patterns, and performance indicators over time. Metrics used for analysis may include event counts by type, time-of-day trends, response times, alert accuracy, and changes in incident frequency. These metrics are used to assess system effectiveness and support operational decision-making.

There won't be a response per say. If someone gets alerted (let's say myself or a team member), it will then be up to the Property Manager to call police as needed (if someone is breaking into the specific building).

Processing occurs in near real-time at the edge or during ingestion, with aggregation and reporting performed on stored event metadata. The scale of processing typically includes multiple deployed devices and cameras generating event records on an ongoing basis. Data retention and processing scope are configurable and aligned with customer-defined policies.

Data analysis may involve combining internal datasets such as event metadata, device information, and location data using non-personal identifiers (e.g., device ID, site ID, timestamp). *The system will not perform biometric identification or identity-based data matching.*

4.0 Legal Scope & Compliance

4.1 Governing Laws: What laws, regulations, rules, or contracts govern (a) the data, (b) the data processing activities, (c) the data sharing?

The Seattle Municipal Code (SMC), the City of Seattle's Data Privacy Ordinance, and other City ordinances grant Finance and Administrative Services (FAS), or their designees, the legal authority to establish, update, and implement policies related to the use of technology for security, asset protection, and public safety. These policies may be enacted with the approval of the City Council and/or the Mayor's Office, depending on the scope and impact of the policy changes. Under the authority provided by the SMC, FAS is authorized to collect and manage data to:

- Protect City assets from theft, vandalism, graffiti, and illegal dumping.
- Ensure public safety and security within parks and recreational facilities.

FAS' data collection practices will comply with the City of Seattle's Data Privacy Ordinance, which establishes guidelines for responsible data collection, use, storage, and sharing to protect individual privacy. FAS will align with City privacy policies, state laws, and any future ordinances that govern the management of collected information.

Additionally, FAS will develop internal policies and procedures to ensure compliance with legal requirements and privacy protections.

LVT adheres to all applicable federal, state, provincial, municipal, and international laws and regulations governing the processing, protection, and privacy of personal information, as detailed in our Data Protection Addendum ("DPA") and Security Compliance Requirements Appendix , which is publicly available and included in our Master Service Level Agreement (MSLA): https://www.lvt.com/msla. And is included as "Exhibit A" for convenience.

4.2 Compliance Measures: What are the compliance measures associated with the use of the technology or data? Who is involved with oversight of requirements defined in 4.1?

Compliance Measures: LVT adheres to all applicable federal, state, provincial, municipal, and international laws and regulations governing the processing, protection, and privacy of personal information, as detailed in our Data Protection Addendum (DPA) and Security Compliance Requirements Appendix, which is publicly available and included in our Master Service Level Agreement (MSLA): https://trust.lvt.com/ (Exhibit A)

Additionally, LVT holds a Washington Limited Energy Electrical contractor license to be used when required.

Authorized Administrator: Customers are responsible for authorizing which specific city personnel have access to the data, conducting periodic audits of their own users activity logs within the LVT Platform and Ensuring the use of LVT technology aligns with the City internal privacy and public disclosure policies.

Third-Party Oversight: Independent Auditors, SOC 2 Type 2 audits and AWS Cloud Service

Provider provides its own layer of oversight regarding physical security where LVT data is hosted. LVT reviews AWS SOC 2 reports annually as part of its Vendor Risk Management Policy.

FAS is able to audit the use of LVT systems and only specific role based access is permitted.

4.3 Records Production Compliance: How is the data and/or associated records (e.g., reports, derivatives, etc.) retrievable in support of public disclosure requirements?

Public disclosure officers are able to pull records as needed.

5.0 Data Security, Protection, & Storage

5.1 Data Access: Who will have access to the data? Who will have access to the technology (if different than who has data access)?

Does LVT have any access to the data? No. LVT is only hosting the data but will not access.

City of Seattle alone has access to data. The City and designated staff will manage which employees have access to data via the LVT Platform and can grant or revoke that access at any time. There is clear auditability around access.

Access to data and technology at LVT is strictly governed by the principles of Role-Based Access Control (RBAC) and Least Privilege. This ensures that only authorized individuals have the specific access they need to perform their jobs.

5.2 Access Authorization: What processes are prerequisites to a user's access of the data or technology (e.g., user authentication, business approvals/sign-off, documentation, etc.)?

City of Seattle folks have access to the footage for 30 days.

Initial system access is established by LVT through the creation of a single client administrator account. The client administrator is responsible for authorizing, creating, and managing all subsequent user accounts, including defining roles and permissions in accordance with the customer's internal policies and least-privilege principles. User access requires authenticated credentials and is limited to the permissions granted by the client administrator. LVT does not authorize or manage end-user access beyond the initial administrator account. Responsibility for approving access to data and system functionality resides entirely with the customer through the designated client administrator and any additional client administrators created by that account. Access activity is logged to support auditing and accountability requirements.

5.3 Secure Storage: Where will the data be stored, and what security measures are in place for the storage of the data?

Data will be stored on vendor cloud. Data is Encrypted and protected at rest. SSO is required to ensure role based access and protection.

5.4 Auditability of Data Access & Data Processing: How will the department ensure that data access and data processing activities are logged and auditable?

Video and picture data is processed in two locations, on the trailers. If filmed, then sent to cloud and partitioned off with role based access. Access activity is logged to support auditing and accountability requirements. FAS will be auditing logs as needed.

6.0 Data Sharing & Disclosure

6.1 Data Sharing Partners: Which entities (internal and external to the City) will be data sharing partners, if any?

Internal Data Sharing: If an incident is recorded, the data may be shared with the City's Law Department for legal review and to determine appropriate enforcement actions.

External Data Sharing: When necessary, captured images may also be provided to law enforcement agencies for investigation and potential prosecution of criminal activities.
To ensure transparency and accountability, FAS is actively working to develop a formal policy update that will define the specific procedures and limitations regarding how data from this technology is shared.

6.2 Purpose for Data Sharing: What is the purpose of sharing data with the identified parties in the context of this effort?

Data sharing is essential to support public safety, protect public assets, and ensure accountability for unlawful activities occurring on FAS properties. Camera footage captured by the LVT system may provide critical evidence of criminal behavior, allowing for appropriate enforcement actions to be taken. In addition to theft, vandalism, graffiti, and illegal dumping, FAS personnel may identify other forms of unlawful activity through camera footage.
When such incidents are documented, they will be reported to the City's Law Department for legal review and, if necessary, shared with law enforcement agencies to assist in investigations and enforcement efforts. By sharing relevant data with law enforcement partners, FAS aims to enhance security, deter future criminal activity, and maintain safety for staff who are working on premises.

6.3 Sharing Restrictions: Describe any restrictions on data use and data access and identify the sources that impose those restrictions.

FAS may share data captured by the LVT system with specific entities inside and external to the City in cases where theft, vandalism, or other criminal activity has been documented.
• Internal Data Sharing: If an incident is recorded, the data may be shared with the City's Law Department for legal review and possibly with Seattle Police Department to determine appropriate enforcement actions.
FAS is actively working to develop a formal policy update that will define the specific procedures and limitations regarding how data from this technology is shared.
This policy will align with privacy regulations, legal requirements, and departmental protocols to ensure responsible handling of all collected data.

Restrictions are governed by the LVT's publicly available standard MSLA and Privacy Policy, which mandate "Purpose Limitation."

- **Purpose Limitation:** Per the MSLA, LVT is restricted from processing Customer Data for any reason other than providing the Services or addressing technical issues.
- **No Data Selling:** The **Privacy Policy** and **MSLA** explicitly prohibit LVT from selling, renting, or leasing Customer Data to third parties.
- **Sub-processor Restrictions:** The **DPA** restricts data access to a specific list of approved sub-processors (e.g., AWS). Any new sub-processor must be vetted and the Customer must be notified.
- **Legal Compulsion:** The **Privacy Policy** states that data will only be disclosed to government authorities when required by a valid legal order (subpoena/warrant), with a commitment to notify the Customer unless legally barred.

Please reference the following resources for additional information.

https://www.lvt.com/legal/msla
https://www.lvt.com/legal/privacy

6.4 Agreement Updates: Please describe the process for reviewing and updating data sharing agreements.

FAS is committed to responsible data management and information sharing in compliance with legal and privacy standards. The department will develop a comprehensive policy outlining the acceptable use, data retention, and information-sharing protocols related to the LVT system.

This policy will specifically address the handling of data collected in cases of theft, vandalism, graffiti, illegal dumping, and other criminal activities occurring on FAS property.
Any new information-sharing agreements, memorandums of understanding (MOUs), expanded uses of the technology, or requests for access—whether from City of Seattle departments or external agencies—will undergo a formal review and approval process. This process will ensure:
• Compliance with applicable laws and regulations, including data privacy and public records laws.
• Alignment with FAS's mission and policies regarding security and public safety.
• Proper protocols for storage, access, and data retention, ensuring that only authorized personnel handle the information.
• Appropriate safeguards are in place to prevent unauthorized access, misuse, or improper disclosure of data.
Any future modifications to access policies or data-sharing agreements will be documented and reviewed periodically to maintain compliance with evolving legal and ethical standards.

6.5 Records of Data Disclosure: How are records that document data disclosure/sharing maintained by the department?

Please describe how these records are documented either by technical functionality or business practices/processes.
FAS will have access to the records with role based, auditable access. FAS will access as needed for investigations or to check logs per policy.

Business Practices & Processes

 Sub-processor Registry: As required by the **DPA**, LVT maintains a current list of all third-party sub-processors who may have access to data. Any changes to this list are documented and communicated to customers.

 Legal Request Tracking: If LVT is legally compelled to disclose data (e.g., via a subpoena, court order, or warrant), the **Privacy Policy** and **MSLA** mandate a formal process. This includes documenting the legal authority for the request and, unless prohibited by law, notifying the Customer of the disclosure.

 Written Certification: Per the **Security Appendix**, LVT can provide written certification or reports upon request to confirm that data has been handled or shared in accordance with the contractual agreements.

 Annual Compliance Audits: LVT undergoes an annual **SOC 2 Type II audit**. The auditors review these disclosure logs (specifically under **Trust Services Criteria for Confidentiality**) to verify that LVT is documenting and restricting data sharing as promised in the MSLA.

Please reference the following resources for additional information

https://www.lvt.com/legal/msla
https://www.lvt.com/legal/privacy

7.0 Data Retention & Destruction

7.1 Data Retention: What are the record retention schedules that govern both the raw data and any derived outputs (e.g., analyses, reports, transformed/cleaned datasets)?

Standard video retention is typically 30 days

MSLA allows for custom retention periods based on specific city or departmental requirements.

7.2 Data Destruction: What mechanisms (technical or process-oriented) are in place to destroy improperly collected data?

Cameras are in designted spaces and should not pick up anything outside of where they are facing. However, LVT ensures the destruction of improperly collected or expired data through the following mechanisms:

Technical Mechanisms

Automated Purge Processes: Internal system scripts identify and permanently remove data that is no longer necessary or has exceeded its retention period.

Physical Media Sanitization: For hardware being decommissioned, LVT utilizes software-based overwriting or physical destruction through a certified third-party vendor.

Process-Oriented Mechanisms

NIST Standards Compliance: All data deletion and media sanitization activities follow the guidelines outlined in **NIST SP 800-**

Annual SOC 2 Verification
These controls are tested annually by independent auditor

7.3 Responsible Staff: Who is responsible for ensuring compliance with data retention and data destruction requirements?

Responsibility for compliance with data retention and destruction is shared across a structured governance hierarchy to ensure accountability. Information Security Officer, Data Owners, IT and DevOps Teams and Legal and Compliance

LVT has automatic destruction schedules for data.
FAS ensure that retention schedules are compliant and met as required.

7.4 Purge Verification: What mechanisms (technical or process-oriented) are in place to ensure that data is properly destroyed after data retention periods have been met?

These technical actions are validated through formalized business practices:

- **NIST Compliance:** When deleting Customer Data, LVT complies with **"NIST Guidelines for Media Sanitization (SP 800-88)"**.
- **Certificates of Destruction:** For any physical media (such as a decommissioned LVT Unit hard drive), LVT requires a **Certificate of Destruction (COD)** from a certified third-party vendor.
- **Written Certification:** Upon request, LVT will provide **written certification** to the Customer that Customer Data has been destroyed in accordance with the Security Appendix.
- **Annual SOC 2 Audit:** An independent third-party auditor annually evaluates LVT's data disposal controls (specifically **Control CC6.1**) to verify that LVT follows its documented procedures for secure disposal.

8.0 Privacy Principles, AI and Privacy Risks, & Controls

8.1 Privacy Risks, Harms, Mitigations, & Controls: What privacy risks exist for the effort, and what are the potential impacts on Seattle residents and/or other data subjects?

Privacy Risks and Mitigation Measures

Multiple privacy risks associated with the collection of data through the LVT system have been identified. The department has implemented strict policies and safeguards to mitigate these risks and ensure compliance with privacy regulations.

Risk: Unauthorized Access to Data

Mitigation: Access to LVT data is restricted exclusively to select staff with role based access. Data is stored on LVT hosting site, accessible only to authorized personnel. Additionally, Law or law enforcement may view footage as needed in the case of an event.
Risk: Retention of Unnecessary or Unrelated Data

Mitigation: Any photos or footage that do not capture theft, vandalism, graffiti, illegal dumping, or other criminal activity are automatically deleted after 30 days retention period.

Risk: Potential Exposure of Non-Involved Individuals or Private Property

Mitigation: Recording is only triggered when illegal activity is detected and confirmed.

Risk: Overuse or feature enablement of surveillance or privacy impacting technology such as ALPR, biometric data collection.

Mitigation: ALPR is disabled. No biometric information collected – object detection to detect and categorize. No analysis on the backend and no training on data collected.

Risk: Lack of Public Awareness About Data Collection

Mitigation: FAS will place clear signage at all monitored locations to inform the public that LVT system is in use. The signage will provide transparency about the system's purpose—deterring and documenting illegal activities such as theft, vandalism, graffiti, and dumping.
By implementing these privacy safeguards, FAS ensures that data collection remains limited, secure, and compliant with legal and ethical standards while balancing public safety and privacy concerns.

Certain aspects of the LVT system may raise public concerns regarding privacy intrusion or potential misuse of personal information. To address these concerns, FAS has implemented clear policies, safeguards, and transparency measures to ensure responsible use of this technology.

Members of the public may worry that their personal images or activities could be captured, stored, or shared inappropriately.

To mitigate these concerns, FAS has established the following privacy protections:

• Strategic Camera Placement: Cameras are installed only in areas with limited public access, strictly monitoring FAS property and avoiding surveillance of adjacent private property.
• Strict Data Retention and Deletion Policies: Any images that do not capture theft, vandalism, or other criminal activities will be deleted within the retention period specified by City clerk. Privacy masks can be applied as needed.

• Access Controls and Security: Only authorized personnel within role based access can access the data.

By implementing these safeguards, FAS ensures that the LVT system serves its intended purpose—to deter and document illegal activities—without compromising public trust, privacy, or civil liberties

AI risks and mitigations:

AI Risk: Sensitive information disclosure through use of AI system models, based on ingestion of sensitive data held by the City.

Mitigation/Control: Contractual requirements are in place to ensure City data will not be used to train or fine-tune the commercial product.

AI Features: AI-Based Video Analytics is utilized on Security Unit cameras to identify objects of interest for the purpose of notifying and alerting security operators of a potential intrusion. The analytics engine is entirely localized on the camera's computational unit.

- The output of the AI-Based Video Analytics are security alerts that include snapshots and a video clip of the event which matched the detection criteria. AI video analytics on the camera will be configured/re-configured by an authorized integration
- This includes detection regions, dwell time, and detection type.
- Controls for making adjustments are not available to end users at this time. These security alerts are customer facing for the customer or monitoring partner if applicable to act on.

LVT relies on open-source AI-based products related to Computer Vision. Open-source computer vision models are leveraged and then tuned based on LVT deployment needs. Neural Network/machine learning/VLM. Object Analytics is just the AI based motion detection plugin on the camera. No learning data is sent to Axis (camera manufacturer) for training or otherwise and is entirely self-contained to the camera. Axis builds their own learning models and releases updates via firmware. The camera recorded footage is on LVT encrypted solid-state drive separate from the camera and is not accessible unless fetched from the LVT platform. The cameras cannot access internet and are incapable of sending any data outside of the network.