skEYEvue Customer Live Video Policy (Rev 08/2023)

At skEYEwatch, we understand the importance of trust and transparency in today's data-driven world. All industries rely heavily on critical infrastructure and the safety of personnel and passengers. We are committed to building strong partnerships with our customers and being transparent about how we collect, use, store, and secure live video data captured by our skEYEvue mobile camera solution.

This policy outlines our practices in detail to ensure you have a clear understanding of how your data is handled. We encourage you to review this policy thoroughly and contact us if you have any questions.

Data Collection

skEYEvue is designed to capture critical visual data to improve safety and operational efficiency in many environments. Here's a breakdown of our data collection practices, with a focus on balancing information needs with privacy:

1. **High-Definition Video:** Our strategically positioned cameras record live video footage in high definition (HD). This high resolution allows for clear observation of road conditions, potential hazards, and surrounding areas, even in challenging lighting conditions.

2. **Focus on Relevant Information:** Camera placement is carefully planned to capture the most relevant visual data for your operations. This may include views of the road ahead, potential obstacles at crossings, and overall situational awareness for the driver.

3. **Privacy by Design with Optional Features:** Our system is designed to minimize the collection of personally identifiable information (PII) by default. Cameras are positioned to avoid capturing faces of people near the vehicle or license plates of passing vehicles. However, we acknowledge the availability of optional features like AI driver behavior cameras that may capture faces in certain situations.

   a) **Optional AI Driver Behavior Cameras:** These cameras, if enabled by your organization, are designed to monitor driver behavior within the vehicle driver area/cab. They may capture facial features to detect signs of fatigue, distraction, or drowsiness.

   b) **Privacy Controls for AI Features:** If you choose to utilize AI driver behavior cameras, skEYEwatch provides tools within our software for you to blur faces before sending video evidence anywhere. This ensures you can leverage the benefits of AI features while maintaining privacy for your personnel.

4. **Audio Recording (Optional):** While skEYEvue primarily focuses on capturing video data, we understand there may be specific situations where audio recording can be beneficial. We can accommodate these needs on a case-by-case basis.

   a) **Standard Operation:** By default, our system does not record any audio conversations taking place within the camera's range, ensuring privacy for drivers and personnel in the vicinity.

   b) **Optional Audio Recording:** If your specific needs require audio recording for certain cameras, please contact skEYEwatch to discuss your requirements. We will work with you to determine the feasibility and any additional security measures needed for audio data collection.

Authorized Use Cases

Live video captured by skEYEvue serves as a valuable tool for enhancing safety and operational efficiency across various driving operations. Here's a breakdown of how authorized personnel can leverage this technology:

1) **Vehicle Drivers/Operators:**

   a) **Real-Time Situational Awareness:** Live video provides a crucial first-person perspective for drivers, allowing them to monitor road conditions in real-time. This includes identifying potential hazards such as debris on the road, approaching pedestrians, etc., enabling them to take necessary precautions to ensure safe operation.

   b) **Improved Visibility in Challenging Conditions:** Inclement weather conditions like fog, heavy rain, or snowfall can significantly reduce visibility. Live video footage can help drivers navigate such situations by providing a clear view of the road ahead, enhancing their ability to operate safely.

2) **Dispatchers and Fleet Managers:**

   a) **Real-Time Fleet Monitoring:** Dispatchers can utilize live video feeds to monitor vehicle movements in real-time. This enables them to make informed decisions regarding scheduling, delays, and route optimization, ensuring smooth and efficient operation.

   b) **Enhanced Jobsite Oversight:** Live video provides valuable insights into yard/onsite job operations, allowing fleet managers to monitor activities remotely. This can be used to optimize resource allocation, identify potential bottlenecks, and ensure efficient loading and unloading procedures.

   c) **Incident Investigation and Analysis:** In case of accidents or incidents, recorded video footage can be a critical tool for investigation. Dispatchers can review the video to understand the sequence of events, identify contributing factors, and implement corrective measures to prevent future occurrences.

3) **Security Personnel:**

   a) **Enhanced Security Monitoring:** Live video can be a valuable asset for security personnel to monitor critical infrastructure and assets. Strategically placed cameras can deter potential trespassing, vandalism, or theft attempts.

   b) **Real-Time Response to Security Incidents:** Security personnel can respond promptly to security breaches or suspicious activities detected through live video feeds. This allows for faster intervention and mitigation of potential threats to personnel, equipment, and cargo.

   c) **Investigation of Security Events:** Recorded video footage can be used by security teams to investigate security breaches and identify perpetrators. This can be crucial for taking appropriate legal action and implementing preventative measures to enhance overall security.

Access Controls:

skEYEwatch prioritizes the security of your live video data by implementing robust access control measures. Here's a detailed breakdown of how we ensure only authorized personnel can access the skEYEvue system:

1) **Restricted Access:** Live video footage is never publicly accessible. Access is strictly limited to authorized personnel within your organization who have been granted explicit permission through a formal approval process. This ensures that only individuals with a legitimate business need can view live video feeds.

2) **Role-Based Access Control (RBAC):** The skEYEvue system utilizes Role-Based Access Control (RBAC). This means user permissions are assigned based on an individual's specific role and responsibilities within your organization. For example:

   a) **Vehicle Operators:** Will have access to live video feeds from their assigned vehicle only. This allows them to monitor their immediate surroundings and ensure safe operation.

   b) **Dispatchers:** May have access to a broader range of cameras across specific routes or regions, enabling them to monitor vehicle movements and manage fleet operations effectively.

   c) **Fleet Managers:** May have the highest level of access, allowing them to view live video feeds from any camera within your network. This facilitates comprehensive oversight and management of your entire fleet camera operation.

   d) **Security Personnel:** May be granted access to specific cameras strategically placed at critical infrastructure points or areas with higher security risks. This allows them to monitor for suspicious activity and respond promptly to security incidents.

Data Retention and Storage:

skEYEwatch understands the importance of balancing data security with regulatory compliance requirements. Here's a detailed breakdown of how we handle data retention and storage for your skEYEvue live video footage:

1) **Data Retention Periods:** The duration we store your live video footage depends on two key factors:

   a) **Industry Regulations:** Different Industries have specific regulations regarding data retention for video surveillance systems. We stay up-to-date on these regulations and ensure our data retention policies comply with all applicable industry standards.

   b) **Your Organization's Policies:** You may have internal data retention policies specific to your organization's needs. We will work with you to determine a data retention period that meets both regulatory requirements and your internal compliance needs. This period can typically range from a few days to several months, depending on the specific regulations and your risk tolerance.

2) **Secure Cloud Storage:** All your live video data is encrypted at rest and in transit using industry-standard encryption protocols. This encryption scrambles the data, making it unreadable to anyone who doesn't possess the decryption key. We store your encrypted video data on secure cloud servers provided by reputable cloud service providers. These providers offer robust security measures, including physical access controls, intrusion detection systems, and regular security audits.

3) **Data Lifecycle Management:** We implement a data lifecycle management process to ensure the secure handling of your video data throughout its entire lifecycle. This includes:

   a) **Classification:** Classifying data based on its sensitivity and associated retention requirements.

   b) **Retention and Archiving:** Storing data securely for the designated retention period.

   c) **Secure Deletion:** After the retention period expires, data is securely overwritten or deleted using industry-approved methods to ensure it cannot be recovered.

4) **Data Access Controls:** Even during storage, access to your video data remains restricted. Only authorized personnel at skEYEwatch with a legitimate business need and your organization's designated skEYEvue administrators will have access to the encrypted data. This ensures an additional layer of security for your sensitive video information.

Your Control Over Your Data:

skEYEwatch is committed to empowering you with control over your data. We understand that your live video footage may contain sensitive information about your operations, and we respect your right to access and manage this data. Here's a detailed breakdown of your rights and how to exercise them:

1) **Data Access Requests:** You have the right to request access to any stored video footage that pertains to your specific fleet operation requirements. This could include footage captured from cameras on vehicles assigned to your team, specific yards you manage, or a particular route your fleets operate on.

   a) **Submission Process:** To submit a data access request, please contact your designated skEYEvue administrator within your organization. They will guide you through a streamlined process and ensure you have the proper authorization to access the requested footage.

   b) **Data Formats:** We will provide the requested video footage in a commonly used and accessible format, unless otherwise specified in your request.

   c) **Fulfillment Timeframe:** We will endeavor to fulfill your data access request within a reasonable timeframe, considering the scope and complexity of the request.

2) **Data Deletion Requests:** Subject to compliance with legal and regulatory requirements, you can submit a request for deletion of your stored video data. This may be relevant for footage captured during specific timeframes or associated with particular incidents that no longer require retention.

   a) **Considerations:** We will carefully assess your deletion request in light of industry regulations and your organization's internal data retention policies. There may be instances where certain footage must be retained for a specific period to comply with legal requirements or ongoing investigations.

   b) **Deletion Process:** Once your deletion request is approved, we will securely erase the designated video data from our storage systems and ensure it cannot be recovered.

   c) **Confirmation:** You will receive confirmation once the deletion process is complete.

3) **Data Retention Preferences:** While industry regulations set minimum data retention periods, you may have preferences for how long you wish to retain your video data beyond those minimums. We encourage you to discuss your data retention preferences with your designated skEYEvue administrator. They can help you determine an appropriate retention period that meets your needs while adhering to compliance requirements.

Security Measures: Safeguarding Your Data with a Multi-Layered Approach

At skEYEwatch, we prioritize the security of your live video data. We implement a comprehensive security framework that utilizes a multi-layered approach to protect your data from unauthorized access, data breaches, and cyberattacks. Here's a detailed breakdown of the security measures we employ:

1) **Network Security:**

   a) **Network Segmentation:** We segment our network infrastructure, creating logical divisions between different systems. This limits the potential damage if a breach occurs in one segment, preventing attackers from gaining access to your critical video data.

   b) **Firewalls and Intrusion Detection/Prevention Systems (IDS/IPS):** We deploy robust firewalls and Intrusion Detection/Prevention Systems (IDS/IPS) to monitor network traffic for suspicious activity. These systems can identify and block unauthorized access attempts, malware intrusions, and other cyber threats.

   c) **Secure Access Controls:** We implement strict access controls to our network. Only authorized personnel and systems have permission to access the network and your video data.

2) **Data Encryption:**

   a) **Encryption in Transit:** All video data is encrypted while being transferred between cameras, the skEYEvue system, and storage servers. This encryption uses industry-standard protocols like AES-256, making the data unreadable to anyone who intercepts it.

   b) **Encryption at Rest:** Your video data remains encrypted even when stored on our secure cloud servers. This ensures that even if an attacker gains access to the storage infrastructure, they cannot access the video footage without the decryption key.

3) **Regular Security Audits and Vulnerability Management:**

   a) **Proactive Penetration Testing:** We conduct regular penetration testing; simulating cyberattacks to identify potential vulnerabilities in our systems. This proactive approach allows us to address weaknesses before they can be exploited by malicious actors.

   b) **Security Patch Management:** We maintain a rigorous security patch management program, ensuring all systems and software components are updated with the latest security patches to address known vulnerabilities.

   c) **Security Awareness Training:** We provide ongoing security awareness training to our employees to educate them on cybersecurity best practices and help them identify and report suspicious activity.

Updates to this Policy:

skEYEwatch is committed to keeping you informed about any changes to this policy. We understand that the data privacy landscape can evolve, and we strive to adapt our practices accordingly. Here's a breakdown of how we will handle updates to this policy:

1) **Prompt Notification:** We reserve the right to update this policy periodically to reflect changes in several areas, including:

   a) **Our data collection and handling practices:** If we introduce new features or functionalities to the skEYEvue system that impact data collection, we will update this policy to reflect those changes.

   b) **Applicable Laws and Regulations:** The legal landscape surrounding data privacy is constantly evolving. We will update this policy to ensure it remains compliant with any new industry regulations or data protection laws.

   c) **Technological Advancements:** As technology advances, we may implement new security measures or data storage solutions. We will update this policy to reflect these advancements and their impact on your data.

2) **Clear Communication Channels:** We will provide clear and timely notification of any material changes to this policy. Here's how you will be informed:

   a) **Direct Notification to Your Organization:** We will endeavor to provide notification of any significant changes to this policy through your designated skEYEvue administrator within your organization. They will be responsible for communicating the updates to relevant personnel within your team.

   b) **Posting on skEYEwatch Website:** The updated policy will also be posted on the skEYEwatch website in a readily accessible location. We recommend you periodically review the policy on our website for any updates.

3) **Your Right to Understand:** We are committed to transparency. If you have any questions or require clarification regarding any changes made to this policy, please don't hesitate to contact us at info@skeyewatch.com. We are here to address your concerns and ensure you understand how any updates may impact your data.

Contact Us:

At skEYEwatch, we understand that you may have questions or concerns regarding this policy and how it pertains to your live video data within the skEYEvue system. We are committed to open communication and addressing your inquiries promptly and transparently. Here's how you can reach us:

Dedicated Support Channels:

1) **skEYEvue Support Website:** We maintain a dedicated skEYEvue Support website with a comprehensive knowledge base and frequently asked questions (FAQs) section. You can

access this website at https://skEYEvue.com and search for answers to your questions. The website may also offer the option to submit a support ticket electronically.

2) **skEYEvue Support Email:** For specific inquiries or if you cannot find the information you need on the website, you can contact our dedicated SkEYEvue Support team directly via email at support@skEYEvue.com. Please include a clear and concise description of your inquiry in your email, along with any relevant details about your organization and the skEYEvue system usage.

3) **skEYEvue Support Phone Line:** If you prefer to speak with a representative directly, you can reach our skEYEvue Support team by phone at 888-998-7787. Our support representatives are available during business hours (8am-5pm) to answer your questions and address your concerns.

Additional Resources:

1) **skEYEwatch Website:** You can also visit the skEYEwatch website at https://skeyewatch.com for more general information about our company, solutions, and commitment to data privacy.

2) **Data Protection Officer (DPO):** For inquiries specifically related to data privacy practices or your rights under this policy, you can contact our designated Data Protection Officer (DPO) at dpo@skEYEwatch.com. The DPO is responsible for overseeing compliance with data protection regulations and can address any concerns you may have regarding your data.

We value your feedback and strive to continuously improve our practices. Do not hesitate to reach out to us if you have any questions, suggestions, or concerns regarding this policy or the skEYEvue system.