2019

BACKBONE
CONSULTANTS

St. Paul Police Department
Body Worn Camera (BWC)
Biennial Audit

Backbone Consultants
50 South Sixth Street, Suite 1360
Minneapolis, MN 55402

Backbone Consultants
50 South Sixth Street, Suite 1360
Minneapolis, MN 55402

Tel: 612-568-7167
Fax: 612-568-7187

info@backboneconsultants.com
www.backboneconsultants.com

November 12, 2019

Body Worn Camera (BWC) Biennial Audit Results

St. Paul Police Department
367 Grove St.
St. Paul, MN 55101

Backbone Consultants planned and performed an audit of the St. Paul Police Department's Body Worn Camera (BWC) program to obtain reasonable assurance that it complies with the 2019 Minnesota Statute 13.825 Portable Recording Systems as of November 12, 2019.

Our testing included on-site interviews and testing of the BWC technology, documentation reviews, and interviews with subject matter experts as it related to record classification, data usage, data destruction, reporting, and authorization to access data.

Backbone Consultants determined that the St. Paul Police Department's Body Worn Camera (BWC) program complies with the 2019 Minnesota Statute 13.825 PORTABLE RECORDING SYSTEMS as it relates to the biennial audit requirements for record classification, data usage, data destruction, reporting and authorization to access data, amongst other requirements.

Because of its inherent limitations, projections of any evaluation of compliance to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate.

DocuSigned by:
Backbone Consultants
7D2E49A1AB3346C...

Backbone Enterprises, Inc.

BWC Biennial Testing Procedures

The following controls document the legislative requirements for St. Paul Police Department's Body Worn Camera program that are defined as in-scope per MN Statute 13.825 subd. 9 - Biennial Audit.

Control #	Process	Control Objective	Testing Procedures	Testing Results
1	Data Classification	Data collected by a portable recording system are private data on individuals or nonpublic data.	Reviewed the BWC policy and identified the current policy does cover data classification on individuals, as required per legislative requirements.	No exceptions noted
2	Data Classification	Data that document the discharge of a firearm by a peace officer in the course of duty other than during training and the killing of an animal that is sick, injured, or dangerous (section 626.553 Subd. 2) are public.	Reviewed the BWC policy and identified the current policy does cover data classification for discharge of a firearm, as required per legislative requirements.	No exceptions noted
3	Data Classification	Data that document the use of force by an officer that results in substantial bodily harm (bodily injury which involves a temporary but substantial disfigurement, or which causes a temporary but substantial loss or impairment of the function of any bodily member or organ, or which causes a fracture of any bodily member), are public.	Reviewed the BWC policy and identified the current policy does cover data classification for use of force, as required per legislative requirements.	No exceptions noted
4	Data Classification	Data are public if a subject of the data requests it be made accessible to the public.	Reviewed the BWC policy and identified the current policy does cover data classification for subjects who request footage to be made public, as required per legislative requirements.	No exceptions noted
5	Data Redaction	Data on a subject who is not a peace officer and who does not consent to the release must be redacted.	Reviewed the BWC policy and identified the current policy does cover redacting on data subjects who don't provided consent.	No exceptions noted
6	Data Redaction	Data on a peace officer whose identity is protected (undercover law enforcement officer) must be redacted.	Reviewed the BWC policy and identified the current policy does cover the need to redact footage of undercover officers with protected identities if/when those officers have been recorded.	No exceptions noted
7	Data Classification	Portable recording system data that are active criminal investigative are confidential or protected nonpublic and governed the Criminal Investigative Data statute (section 13.82, subdivision 7).	Reviewed the BWC policy and identified the current policy does cover data classification for active criminal investigations, as required per legislative requirements.	No exceptions noted
8	Data Classification	Portable recording system data that are inactive criminal investigative data are public as governed by this data classification section.	Reviewed the BWC policy and identified the current policy does cover data classification for inactive criminal investigations, as required per legislative requirements.	No exceptions noted

Control #	Process	Control Objective	Testing Procedures	Testing Results
9	Data Classification	Data is public regarding the final disposition of any disciplinary action together with the specific reasons for the action and data documenting the basis of the action, excluding data that would identify confidential sources who are employees of the public body.	Reviewed the BWC policy and identified the current policy does cover data classification for disciplinary action.	No exceptions noted
10	Data Classification	Data that are not public data under other provisions of this chapter retain that classification.	Reviewed the BWC policy and identified the current policy does state that data which are not public data under other provisions retain that classification.	No exceptions noted
11	Data Redaction	A law enforcement agency may redact or withhold access to portions of data that are public under this subdivision if those portions of data are clearly offensive to common sensibilities.	Reviewed the BWC policy and identified the current policy does detail the SPPDs authorization to withhold access to public footage if deemed offensive.	No exceptions noted
12	Data Classification	Tennessen warning (Section 13.04, subdivision 2) does not apply to collection of data classified by this subdivision.	Reviewed the BWC policy and identified the current policy does document that the Tennessen warning does not apply to collection of BWC data.	No exceptions noted
13	Data Classification	The person bringing the action to challenge a determination to withhold access to portion of data must give notice of the action to the law enforcement agency and subjects of the data, if known.	Reviewed the BWC policy and identified the current policy documents the rights of a person to challenge a determination and their responsibility to provide notice.	No exceptions noted
14	Notice	The law enforcement agency must give notice to other subjects of the data, if known, who did not receive the notice from the person bringing the action	Reviewed the BWC policy and identified the current policy does address its obligation to provide notice to known data subjects in the event a video is challenged in district court.	No exceptions noted
15	Data Classification	The right of a defendant in a criminal proceeding to obtain access to portable recording system data under the Rules of Criminal Procedure is not affected by section related to withholding access or redacting portion of data that is clearly offensive to common sensibilities.	Reviewed the BWC policy and identified the current policy does detail the right of a defendant to access footage deemed offensive.	No exceptions noted
16	Public Comment	Section 626.8473 requires a law enforcement agency to allow for public comment and to create written policies and procedures before it purchases body cams or implements a body cam program. Such policies and procedures must be in place by January 15, 2017.	Reviewed documentation pertaining to the public comment meeting and confirmed a meeting for public comment input took place on November 16, 2016.	No exceptions noted

Control #	Process	Control Objective	Testing Procedures	Testing Results
17	Data Retention	Body cam data that are not active or inactive criminal investigative data must be retained for at least 90 days.	Reviewed the BWC policy and the Evidence.com data retention settings and identified that all data categories at Evidence.com have data retention settings configured for a minimum of 90 days, and are configured according to the data retention policy.	No exceptions noted
18	Data Retention	Body cam data must be destroyed according to the agency's record retention schedule approved pursuant to section 138.17 (retention schedule approved by the head of the governmental unit or agency having custody of the records and the MN Records Disposition Panel)	Evaluated the BWC policy and the evidence.com data retention settings and identified that all data categories at evidence.com have data retention settings configured for a minimum of 90 days, and configured according to the data retention policy. Confirmed data is destroyed per CJIS standards once retention schedule is met,	No exceptions noted
19	Data Retention	Body cam data must be retained for at least one year if they document an incident where an officer discharges a firearm in the course of duty other than the exceptions noted in section 626.553 Subd 2 (training and the killing of an animal that is sick, injured, or dangerous,)	Reviewed the BWC policy and the Evidence.com retention settings for discharge of a firearm and confirmed the retention is set to 7 years.	No exceptions noted
20	Data Retention	Body cam data must be retained for at least one year if they document the use of force by an officer that results in substantial bodily harm.	Reviewed the BWC policy and the evidence.com retention settings for Use of Force and confirmed the retention is set to 7 years.	No exceptions noted
21	Data Retention	Body cam data must be retained for at least one year if a formal complaint is made against an officer related to an incident.	Reviewed the BWC policy and the Evidence.com retention settings for formal complaints and confirmed the retention settings are set to an indefinite hold (manual deletion only).	No exceptions noted
22	Data Retention	If a subject of the data submits a written request to retain the recording, the data must be retained for the time period requested, of up to an additional 180 days beyond the applicable retention period.	Reviewed the BWC policy and identified the current policy does address its obligation to retain data for 180 days if written requests are submitted. A process has been defined on how to process and manage these requests is also covered within the BWC policy.	No exceptions noted
23	Data Retention	The law enforcement agency shall notify the requester that the recording will be destroyed when the requested time elapsed unless a new request is made.	Reviewed the BWC policy and confirmed the current policy does address its obligation to notify the requestor their retention request period is about to expire and is subject to deletion. A process is defined on how the records unit will engage the requestor prior to deletion of the record(s).	No exceptions noted
24	Data Retention	A government entity may retain a recording for as long as reasonably necessary for possible	Reviewed the BWC Policy and confirmed the current policy does properly cover SPPD's right	No exceptions noted

Control #	Process	Control Objective	Testing Procedures	Testing Results
		evidentiary or exculpatory use related to the incident with respect to which the data were collected.	to retain recordings for as long as reasonably necessary.	
25	Access by Data Subjects	An individual who is the subject of portable recording system data can have access to the data, including data on other individuals who are the subject of the recording.	Reviewed the BWC Policy and confirmed the current policy does cover the rights of data subjects	No exceptions noted
26	Access by Data Subjects	If the individual requests a copy of the recording, data on other individuals who do not consent to its release must be redacted from the copy.	Reviewed the BWC Policy and confirmed the current policy does cover the requirement to redact individuals who do not consent to the release of footage	No exceptions noted
27	Access by Data Subjects	The identity and activities of an on-duty peace officer engaged in an investigation or response to an emergency, incident, or request for service may not be redacted, unless the officer's identity is subject to protection under section 13.82, subdivision 17, clause (a) (when access to the data would reveal the identity of an undercover law enforcement officer).	Reviewed the BWC Policy and confirmed the current policy does address footage of officers are not to be redacted, unless protected per 13.82 sudb. 17.	No exceptions noted
28	Inventory of Portable Recording System Technology	A law enforcement agency that uses a portable recording system must maintain the following information, which is public data: (1) the total number of recording devices owned or maintained by the agency; (2) a daily record of the total number of recording devices actually deployed and used by officers and, if applicable, the precincts in which they were used; (3) the policies and procedures for use of portable recording systems required by section 626.8473; and (4) the total amount of recorded audio and video data collected by the portable recording system and maintained by the agency, the agency's retention schedule for the data, and the agency's procedures for destruction of the data.	Reviewed the reporting capabilities of evidence.com and confirmed the total number of recording devices owned or maintained by the agency, daily record of the total number of recording devices deployed and used by officers, and the total amount of recorded audio and video data collected by the portable recording system and maintained by the agency are all reportable from the system. Confirmed the remaining items are addressed in the BWC policy and CJIS whitepaper.	No exceptions noted
29	Portable Recording Systems Adoption; Written Policy Required	The chief officer of every state and local law enforcement agency that uses or proposes to use a portable recording system must establish and enforce a written policy governing its use.	Reviewed and confirmed a written BWC policy is in place and does govern BWC use.	No exceptions noted
30	Portable Recording Systems Adoption; Written Policy Required	The written policy must be posted on the agency's Web site, if the agency has a Web site.	Confirmed the current BWC policy is available on the St. Paul Police Department's website.	No exceptions noted

Control #	Process	Control Objective	Testing Procedures	Testing Results
31	Portable Recording Systems Adoption; Written Policy Required	At a minimum, the written policy must incorporate the following: (1) the requirements of section 13.825 and other data classifications, access procedures, retention policies, and data security safeguards that, at a minimum, meet the requirements of chapter 13 and other applicable law; (2) procedures for testing the portable recording system to ensure adequate functioning; (3) procedures to address a system malfunction or failure, including requirements for documentation by the officer using the system at the time of a malfunction or failure; (4) circumstances under which recording is mandatory, prohibited, or at the discretion of the officer using the system; (5) circumstances under which a data subject must be given notice of a recording; (6) circumstances under which a recording may be ended while an investigation, response, or incident is ongoing; (7) procedures for the secure storage of portable recording system data and the creation of backup copies of the data; and (8) procedures to ensure compliance and address violations of the policy, which must include, at a minimum, supervisory or internal audits and reviews, and the employee discipline standards for unauthorized access to data contained in section 13.09.	Reviewed BWC documentation and confirmed the following requirements were present and complete in the written policy, procedure, or vendor documentation: (1) the requirements of section 13.825 and other data classifications, access procedures, retention policies, and data security safeguards, (2) procedures for testing the portable recording system to ensure adequate functioning; (3) procedures to address a system malfunction or failure, including requirements for documentation by the officer using the system at the time of a malfunction or failure; (4) circumstances under which recording is mandatory, prohibited, or at the discretion of the officer using the system; (5) circumstances under which a data subject must be given notice of a recording; (6) circumstances under which a recording may be ended while an investigation, response, or incident is ongoing; (7) procedures for the secure storage of portable recording system data and the creation of backup copies of the data; (8) procedures to ensure compliance and address violations of the policy, which must include, at a minimum, supervisory or internal audits and reviews, and the employee discipline standards for unauthorized access to data contained in section 13.09.	No exceptions noted
32	Data Protection	The responsible authority shall: (1) establish procedures to assure that all data on individuals is accurate, complete, and current for the purposes for which it was collected; (2) establish appropriate security safeguards for all records containing data on individuals, including procedures for ensuring that data that are not public are only accessible to persons whose work assignment reasonably requires access to the data, and is only being accessed by those persons for purposes described in the procedure; and (3) develop a policy incorporating these	Reviewed BWC documentation and confirmed the following requirements were present and complete in the written policy, procedure, or vendor documentation: (1) establish procedures to assure that all data on individuals is accurate, complete, and current for the purposes for which it was collected; (2) establish appropriate security safeguards for all records containing data on individuals, including procedures for ensuring that data that are not public are only accessible to persons whose work assignment reasonably requires access to the data, and is only being	No exceptions noted

Control #	Process	Control Objective	Testing Procedures	Testing Results
		procedures, which may include a model policy governing access to the data if sharing of the data with other government entities is authorized by law. (4) When not public data is being disposed of, the data must be destroyed in a way that prevents its contents from being determined.	accessed by those persons for purposes described in the procedure; and 3) develop a policy incorporating these procedures, which may include a model policy governing access to the data if sharing of the data with other government entities is authorized by law. (4) When not public data is being disposed of, the data must be destroyed in a way that prevents its contents from being determined.	
33	Penalties	Procedures to ensure compliance and address violations of the policy, which must include the employee discipline standards for unauthorized access to data contained in section 13.09. (a) Any person who willfully violates the provisions of this chapter or any rules adopted under this chapter or whose conduct constitutes the knowing unauthorized acquisition of not public data, as defined in section 13.055, subdivision 1, is guilty of a misdemeanor.	Reviewed the BWC policy and confirmed the current policy does mention disciplinary actions, which may include termination, for employees who access unauthorized data.	No exceptions noted
34	Penalties	Procedures to ensure compliance and address violations of the policy, which must include the employee discipline standards for unauthorized access to data contained in section 13.09. (b) Willful violation of this chapter, including any action subject to a criminal penalty under paragraph (a), by any public employee constitutes just cause for suspension without pay or dismissal of the public employee.	Reviewed the BWC policy and confirm disciplinary actions are covered in the policy for unauthorized access to data.	No exceptions noted
35	Use of Agency-Issued Portable Recording Systems	While on duty, a peace officer may only use a portable recording system issued and maintained by the officer's agency in documenting the officer's activities.	Reviewed the BWC policy and confirm it mandates officers may only use department issued devices and is in line with the legislative requirements.	No exceptions noted
36	Data Breach Notification	A government entity that collects, creates, receives, maintains, or disseminates private or confidential data on individuals must disclose any breach of the security of the data following discovery or notification of the breach.	Reviewed the BWC policy and confirmed that data breach notification is properly addressed in the current policy.	No exceptions noted
37	Data Breach Notification	Written notification must be made to any individual who is the subject of the data and whose private or confidential data was, or is reasonably believed to have been, acquired by an unauthorized person and must inform the individual that a report will be prepared.	Reviewed the BWC policy and confirmed that written notification is properly addressed in the current policy.	No exceptions noted

Control #	Process	Control Objective	Testing Procedures	Testing Results
38	Data Breach Notification	Upon completion of an investigation into any breach in the security of data the responsible authority shall prepare a report on the facts and results of the investigation. If the breach involves unauthorized access to or acquisition of data by an employee, contractor, or agent of the government entity, the report must at a minimum include: (1) a description of the type of data that were accessed or acquired; (2) the number of individuals whose data was improperly accessed or acquired; (3) if there has been final disposition of disciplinary action for purposes of section 13.43, the name of each employee determined to be responsible for the unauthorized access or acquisition, unless the employee was performing duties under chapter 5B; and (4) the final disposition of any disciplinary action taken against each employee in response.	Reviewed the BWC policy and confirmed that data breach notification is properly addressed in the current policy.	No exceptions noted
39	Security Assessments and data warehouse; Notice Required for Certain Disclosures	At least annually, each government entity shall conduct a comprehensive security assessment of any personal information maintained by the government entity	Personal information is defined under section 325E.61, subdivision 1, paragraphs (e) and (f). Per the defined definition, documented below, evidence.com does not qualify as storing personal information and thus does not need to meet the requirement of an annual security assessment.	No exceptions noted
40	Authorization to Access Data	The responsible authority for a law enforcement agency must establish written procedures to ensure that law enforcement personnel have access to the portable recording system data that are not public only if authorized in writing by the chief of police, sheriff, or head of the law enforcement agency, or their designee, to obtain access to the data for a legitimate, specified law enforcement purpose.	Reviewed the Access control procedure for the SPPD BWC program and confirmed the documented procedures sufficiently meet the requirements defined in the legislation.	No exceptions noted
41	Authorization to Access Data	Review the user access list to the portable recording system and ensure the access is appropriate and has been approved in writing according to the agency written procedure.	Extracted a list of all users from evidence.com and validated if all users had proper written approvals and if the approved roles match the roles defined within evidence.com. Confirmed all users had a documented written approval and their access levels within evidence.com matched the role levels they were approved.	No exceptions noted

Control #	Process	Control Objective	Testing Procedures	Testing Results
42	Sharing Among Agencies	Portable recording system data that are not public may only be shared with or disseminated to another law enforcement agency, a government entity, or a federal agency upon meeting the standards for requesting access to data as provided in subdivision 7	Reviewed the BWC Policy and confirmed the policy does define obligations relating to sharing with other agencies and does include the requirement they follow the Minnesota Data Governance Practices Act.	No exceptions noted
43	Sharing Among Agencies	If data collected by a portable recording system are shared with another state or local law enforcement agency under this subdivision, the agency that receives the data must comply with all data classification, destruction, and security requirements of this section.	Reviewed the BWC Policy and confirmed it properly addresses SPPD's responsibility to comply with data classification, access, destruction, use, retention and security requirements for data obtained from other agencies.	No exceptions noted
44	Sharing Among Agencies	Portable recording system data may not be shared with, disseminated to, sold to, or traded with any other individual or entity unless explicitly authorized by this section or other applicable law.	Reviewed the BWC Policy and confirmed it addresses that footage may not be shared with, disseminated to, sold to, or traded with any other individual or entity unless explicitly authorized by MN Statute 13.825 or other applicable law.	No exceptions noted
45	Data Retention	A law enforcement agency must maintain records showing the date and time portable recording system data were collected and the applicable classification of the data.	Reviewed the exported the body camera logs and confirmed evidence.com sufficiently captures detailed logs/metrics to satisfy legislative requirements.	No exceptions noted
46	Notification to BCA	Within ten days of obtaining new surveillance technology that expands the type or scope of surveillance capability of a portable recording system device beyond video or audio recording, a law enforcement agency must notify the Bureau of Criminal Apprehension that it has obtained the new surveillance technology	Confirmed no other new surveillance technologies, beyond voice and video, are in operation other than the BWC program. Reporting to the BCA is not required. Policy does address their obligation to notify the BCA upon obtaining new surveillance technologies.	No exceptions noted
47	Notification to BCA	The notice must include a description of the technology and its surveillance capability and intended uses. The notices are accessible to the public and must be available on the bureau's Web site.	Confirmed no other new surveillance technologies, beyond voice and video, are in operation other than the BWC program. Reporting to the BCA is not required. The BWC Policy does address the departments obligations and notice requirements in the event new surveillance technology is obtained.	No exceptions noted
48	Portable Recording System Vendor	Vendors that provide portable recording services to a government entity are subject to all of the requirements of the portable recording system statute as if it were a government entity.	Reviewed Axon's SOC2 and Privacy Level Statement to note compliance with applicable portable recording system state statues.	No exceptions noted
49	Portable Recording System Vendor	A portable recording system vendor that stores portable recording system data in the cloud must protect the data in accordance with the security requirements of the United States Federal Bureau of Investigation Criminal Justice	Reviewed Axon's CJIS whitepaper which states evidence.com is compliant with CJIS Security Policy v5.7.	No exceptions noted

Control #	Process	Control Objective	Testing Procedures	Testing Results
		Information Services Division Security Policy 5.4 or its successor version.		
50	Portable Recording System Vendor	All contracts entered into by a government entity must include a notice that the requirements of this subdivision apply to the contract. Failure to include the notice in the contract does not invalidate the application of this subdivision.	Reviewed the Axon contractual agreement and validated that contract with Axon references adherence to Minnesota § 13.05.	No exceptions noted
51	Portable Recording System Vendor	This subdivision does not create a duty on the part of the private person to provide access to public data to the public if the public data are available from the government entity	Reviewed the Axon contractual agreement and validated that contract with Axon references adherence to Minnesota § 13.05.	No exceptions noted