INDEPENDENT AUDIT REPORT

Chief Erik Fadden
Plymouth Police Department
3400 Plymouth Blvd.
Plymouth, MN 55447

Dear Chief Fadden:

An independent audit of the Plymouth Police Department's Portable Recording System (body-worn cameras (BWCs)) was conducted on October 14, 2025. The objective of the audit was to verify Plymouth Police Department 's compliance with Minnesota Statutes §§13.825 and 626.8473.

Data elements the audit includes:

Minnesota Statute §13.825

- Data Classification
- Retention of Data
- Access by Data Subjects
- Inventory of Portable Recording System Technology
- Use of Agency-Issued Portable Recording Systems
- Authorization to Access Data
- Sharing Among Agencies

Minnesota Statute §626.8473

- Public Comment
- Body-worn Camera Policy

The Plymouth Police Department is located in Hennepin County and employs eighty-two (82) peace officers. The Plymouth Police Department utilizes WatchGuard BWCs and Evidence Library Management software. BWC data is stored on a local file server and in the Motorola WatchGuard Cloud. The audit covers the time period April 1, 2022, through July 31, 2024.

Audit Requirement: Data Classification

Determine if the data collected by BWCs are appropriately classified.

Plymouth Police Department BWC data is presumptively private. All data collected during the audit period is classified as private or non-public data. The Plymouth Police Department had no incidents of the discharge of a firearm by a peace officer, use of force that resulted in substantial bodily harm, requests from data subjects for the data to be made accessible to the public, or court orders directing the agency to release the BWC data to the public.

No discrepancies noted.

Audit Requirement: Retention of Data

Determine if the data collected by BWC's are appropriately retained and destroyed in accordance with statutes.

The Plymouth Police Department utilizes the General Records Retention Schedule for Minnesota Cities and agency specified retention periods in WatchGuard. At the conclusion of a BWC recording, officers assign a WatchGuard category type. Each category has an associated retention period. Upon reaching the retention date, data is systematically deleted.

Event log reports of BWC data collected and deleted during the audit period were produced. Records from the purged event log report were reviewed and the date the data was collected was verified against the purge date. Several records were deleted in less than the minimum ninety (90) days required by statute when transitioning data storage from the local file server to the cloud. The issue was immediately rectified, and all other records were deleted in accordance with the record retention schedule and were maintained for at least the minimum ninety (90) days required by statute.

Active BWC data is accessible in the WatchGuard Evidence Library. The server and cloud event logs maintain a listing of all active and deleted BWC data with associated meta data.

The Plymouth Police Department received no requests from data subjects to retain BWC data beyond the applicable retention period during the audit period.

Supervisors monitor BWC data for proper categorization to ensure BWC data are appropriately retained and destroyed.

Discrepancy noted.

Audit Requirement: Access by Data Subjects

Determine if individuals who are the subject of collected data have access to the data, and if the data subject requests a copy of the data, other individuals who do not consent to its release must be redacted.

BWC data is available to data subjects, and access may be requested by submission of a City of Plymouth Information Disclosure Request form. During the audit period, the Plymouth Police Department received both requests to view and requests for copies of BWC video from data subjects. Data subjects who had not consented to the release of data were redacted. Requests for BWC data are documented in an Excel spreadsheet and in the records management system.

No discrepancies noted.

Audit Requirement: Inventory of Portable Recording System Technology

*Determine the total number of recording devices owned and maintained by the agency; a daily record of the total number of recording devices actually deployed and used by officers, the *

policies and procedures for use of portable recording systems by required by section 626.8473; and the total amount of recorded audio and video collected by the portable recording system and maintained by the agency, the agency's retention schedule for the data, the agency's procedures for destruction of the data, and that the data are available to the public.

Plymouth Police Department's BWC inventory consists of one hundred four (104) devices. Device inventory is maintained in Evidence Library and an Excel spreadsheet.

Plymouth Police Department's BWC policy governs the use of portable recording systems by peace officers while in the performance of their duties. The policy requires officers to conduct a function test of their issued BWC at the beginning of each shift to make sure the device is operating properly. Officers noting a malfunction during testing or at any other time are required to promptly report the malfunction to their supervisor and obtain a functioning device as soon as reasonably practical.

Peace officers were trained on the use of the BWC system during implementation. Newly hired officers are trained as part of their field training program.

Officers working on randomly selected dates, and randomly selected calls for service, were verified against the event log reports and confirmed that BWCs are being deployed and officers are wearing and activating their BWCs. A comparison between the total number of BWC videos created per quarter and total calls for service shows a consistent collection of BWC data.

The total amount of active data is accessible in the WatchGuard Evidence Library. The total amount of active and deleted data is documented in the event log reports.

The Plymouth Police Department utilizes the General Records Retention Schedule for Minnesota Cities and agency specified retention in WatchGuard. BWC video is fully deleted upon reaching the scheduled deletion date. In accordance with CJIS media destruction guidelines, server data is overwritten three times. Meta data is maintained on the local file server and the cloud. BWC data is available upon request, and access may be requested by submission of a Plymouth Police Department Information Disclosure Request form.

No discrepancies noted.

Audit Requirement: Use of Agency-Issued Portable Recording Systems

Determine if peace officers are only allowed to use portable recording systems issued and maintained by the officer's agency.

The Plymouth Police Department's BWC policy states that officers will use only department-issued BWCs in the performance of official duties for the agency or when otherwise performing authorized law enforcement services as an employee of the department.

No discrepancies noted.

Audit Requirement: Authorization to Access Data

Determine if the agency complies with sections 13.05, Subd. 5, and 13.055 in the operation of portable recording systems and in maintaining portable recording system data.

Supervisors conduct monthly random reviews of BWC videos to ensure proper labeling and that BWCs are being utilized in compliance with policy.

Nonpublic BWC data is only available to persons whose work assignment reasonably requires access to the data. User access to BWC data is managed by the assignment of group roles and permissions in WatchGuard. Permissions are based on staff work assignments. Access to Evidence Library is password protected and requires dual authentication.

The BWC policy governs access to BWC data. The BWC policy states that no employee may have access to the Department's BWC data except for legitimate law enforcement or data administration purposes. Agency personnel are prohibited from accessing BWC data for nonbusiness reasons and from sharing the data for non-law-enforcement related purposes. Access to data is captured in the audit log. The BWC policy states that the unauthorized access to or disclosure of BWC data may constitute misconduct and subject individuals to disciplinary action and criminal penalties pursuant to Minn. Stat. § 13.09.

When BWC data is deleted, its contents cannot be determined. The Plymouth Police Department has had no security breaches. A BCA CJIS security audit was conducted in July of 2024.

No discrepancies noted.

Audit Requirement: Sharing Among Agencies

Determine if non-public BWC data is shared with other law enforcement agencies, government entities, or federal agencies.

The Plymouth Police Department's BWC policy allows for the sharing of data with other law enforcement agencies, prosecutors, courts, and other criminal justice entities as provided by law. The Plymouth Police Department requires a written request from law enforcement agencies seeking access to BWC data. Sharing of data is documented in an Excel spreadsheet and the records management system.

No discrepancies noted.

Audit Requirement: Biennial Audit

*Determine if the agency maintains records showing the date and time the portable recording system data were collected, the applicable classification of the data, how the data are used, and *

whether data are destroyed as required.

WatchGuard Evidence Library and the event log reports document the date and time portable recording system data was collected and deleted. The WatchGuard audit log, Excel spreadsheet, and the Records Management System document how the data are used and shared.

No discrepancies noted.

Audit Requirement: Portable Recording System Vendor

Determine if portable recording system data stored in the cloud, is stored in accordance with security requirements of the United States Federal Bureau of Investigation Criminal Justice Information Services Division Security Policy 5.4 or its successor version.

During the audit period, Plymouth Police Department's BWC data was stored both on a local file server and in the Motorola WatchGuard Cloud. The server is located in a secure area with limited access. The server is password protected and requires dual authentication.

A Motorola Solutions CJIS Compliance White paper outlines the specific security policies and practices for Motorola Solutions and how they are compliant with the CJIS Security Policy. Motorola has performed statewide CJIS-related vendor requirements in Minnesota. Motorola maintains CJIS certification for personnel who are required to complete Level 4 CJIS Security Training upon assignment and annually thereafter.

No discrepancies noted.

Audit Requirement: Public Comment

Determine if the law enforcement agency provided an opportunity for public comment before it purchased or implemented a portable recording system and if the governing body with jurisdiction over the budget of the law enforcement agency provided an opportunity for public comment at a regularly scheduled meeting.

The Plymouth Police Department solicited for public comment by social media release on February 6, 2019. The Plymouth City Council held a public hearing at their March 12, 2019, Council Meeting.

No discrepancies noted.

Audit Requirement: Body-worn Camera Policy

Determine if a written policy governing the use of portable recording systems has been established and is enforced.

The Plymouth Police Department established and enforces a BWC policy. The policy was compared to the requirements of Minn. Stat. § 626.8473. The policy included all minimum

requirements of Minn. Stat. § 626.8473, Subd. 3(b). The Plymouth Police Department's BWC policy is posted on the agency's website.

No discrepancies noted.

This report was prepared exclusively for the City of Plymouth and Plymouth Police Department by Lynn Lembcke Consulting. The findings in this report are impartial and based on information and documentation provided and examined.

Dated: November 4, 2025

Lynn Lembcke Consulting

Lynn Lembcke

Lynn Lembcke