

<b>Title:</b>	<b>COMPENSATORY TIME</b> <b>[COMP-TIME]</b>	<b>Order #</b>	<b>1-147.1 [a]</b>
<b>New / Amends / Resc:</b>	New Amended	<b>Page:</b>	01 of 02
<b>Approved by:</b>	Chief Ken K. Antolik	<b>Officer Signature:</b>	
<b>Effective Date:</b>	July 1, 2016		
<b>Review Date:</b>			

### Purpose

The purpose of this policy is to establish consistency across state agencies on compensatory time usage and payment and to ensure conformity with the federal Fair Labor Standards Act (FLSA).

### Eligibility

All BHPD employees are subject to this policy. The Chief of Police or his / her designee shall determine whether FLSA covered positions receive overtime compensated or compensatory time.

### Definitions

**FLSA Compensatory Time:** Compensatory time worked beyond 40 hours in a standard workweek. FLSA covered positions accrue overtime at time and a half (1.5). (Note that part-time employee positions are not eligible for alternative work schedules that exceed 40 hours in a given week.)

**Compensatory Time:** Compensatory time earned at straight time regardless of FLSA status as follows:

For hours worked between 37.5 and 40.0 hours in a standard workweek.

For covered time worked by essential BHPD employees during Severe Weather Conditions and Emergencies

Part-Time employees are not eligible for compensatory time. Part-Time employees are paid on

an hourly basis not to exceed 40 hours per pay period.

### Policy

There is a cap on compensatory time of 240 payable hours. 240 payable hours is equal to 160 hours at time and a half.

a. Worked between 37.5 and 40 in one pay week is straight time

b. Worked in excess of 40 in one pay week is time and a half

Employees who request to attend conferences, seminars or other training during weekends or after their regularly scheduled day are not entitled to compensatory time unless approved by the Chief of Police or his designee. Employees may flex their work time around the event with the approval of their supervisor as stated above. If the Chief of Police requires the conferences, seminars or other training, then an employee may be entitled to compensatory time. The hours the employee would be compensated and would exclude the time that the individual would normally travel to his/her job.

All overtime services performed beyond the standard workweek must be approved in advance whenever possible. Compensation, either in the form of cash payment or compensatory time, must be determined in advance between the employee and the



designated authority within the agency. Supervisors should authorize overtime only when in the best interest of the department. Overtime should not be authorized for any assignment, which could have been completed during regular working hours. In emergencies, if prior approval is not obtained, the employee must notify his / her immediate supervisor and or the Chief of Police the reasoning for over-time, or request for comp-time. Any BHPD employee who chooses to perform overtime services that are not authorized or required, in advance, by someone within his/her chain of command may be subject to disciplinary/corrective action.

Supervisor(s) or the Chief's designee should encourage flex time (within the 7 day period earned) to reduce compensation for overtime service and should be judicious in granting the use of annual leave and compensatory time use so as to minimize the eligibility for compensation for overtime service. However, supervisor(s) or the Chief's designee should not require that time be flexed in lieu of use of scheduled sick leave, if used appropriately, regardless of how such use affects compensation for overtime service.

An employee may not earn compensatory time while on paid leave (annual leave, sick leave, compensatory time, etc.).

Accumulated compensatory time should be used as soon as possible after accrual provided such usage does not disrupt the operations of the agency. The

approval process for the use of compensatory time should be similar to the approval process for annual leave. Approval for the usage of compensatory time should not be unreasonably withheld.

Compensatory time may never be taken before it is earned.

All supervisors shall be held accountable for ensuring that an official record is maintained of all time earned and used, including overtime and compensatory time. Employees are responsible for knowing their own compensatory accrual and usage thereof.

For record keeping purposes, compensatory time (unless otherwise specified in this policy) shall be accrued and taken in quarter hour intervals. Less than seven minutes into the quarter is not counted, but seven minutes or more is rounded up to the next quarter hour.

An employee shall not be approved to work overtime that would exceed a balance of 80 hours per pay period without the approval of the Chief of Police (or his/her designee) excluding Court and exigent circumstances i.e., death investigations, arrests and incidentals.

As long as all other applicable laws, rules and regulations are not violated, agencies may make more restrictive compensatory time policies in order to meet operational needs, but cannot make less restrictive policies.

POLICE DEPARTMENT





**BERWYN HEIGHTS POLICE**

**Chief Ken K. Antolik**

# Memo

**To:** All Officer and Civilians  
**From:** Chief K. Antolik  
**CC:**  
**Date:** March 7, 2016  
**Re:** Compensation Time Policy

---

You may be familiar with the term "comp time," which refers to the practice of allowing an employee to take extra time off from work after a long week, instead of being paid overtime wages. The FLSA requires that employers must provide hourly workers compensatory time equal to 1.5 times the amount of overtime they work.

According to the federal Fair Labor Standards Act, or FLSA, hourly workers must receive the overtime rate when they put in more than 40 hours in a payroll week. The employer is prohibited from granting the worker time off during a different payroll week instead of granting overtime pay. The employer cannot average an employee's hours over two payroll weeks, even if the weeks both fall in the same pay period.

When an employee works, say, 50 hours in a payroll week, he or she must be paid in the following way: 40 hours of regular time and 10 hours of overtime. The overtime is always calculated at 1.5 times the worker's average pay rate for the payroll week. For example, if Dan works 50 hours in the first week of the payroll period. His employer pays every two weeks. Next week, Dan works 25 hours and takes 15 hours of comp time. This would be illegal unless he is willing and agreed to do so.

Compensation Time Record can be found on the BHPD server under Comp Time Record. See attached policy.



**Per Pay Period**



NAME DET/SGT Ken Antolik #1425 PAY PERIOD ENDING - 05/02/09

.25	=	.38	1.25	=	1.88	2.25	=	3.38
.50	=	.75	1.50	=	2.25	2.50	=	3.75
.75	=	1.13	1.75	=	2.63	2.75	=	4.13
1.00	=	1.50	2.00	=	3.00	3.00	=	4.50

<b>S i g n a t u r e</b>	<b>D a t e</b>



<b>Title:</b>	<b>COMMUNITY RELATIONS</b>	<b>Order #</b>	<b>1-200</b>
<b>New/Amends/Resc:</b>	New	<b>Page:</b>	01
<b>Approved by:</b>	Chief Ken K. Antolik	<b>Officer Signature:</b>	
<b>Effective Date:</b>	July 01, 2011		
<b>Review Date:</b>			

### 1-200 COMMUNITY RELATIONS

A citizen's encounter with the police can be frightening or emotionally painful experience and under these circumstances the risk of misunderstanding is very great. Contacts between employees and citizens may occur in emotionally-charged situations which can seriously impact the situation.

Employees should strive to develop a climate within the community supportive of collective police community efforts toward common goals of peace, safety, and security. The citizens of Berwyn Heights are supportive of the Police Department and work together with its officer to accomplish these goals. This relationship is to be valued and encourage.

<b>Title:</b>	<b>INDIVIDUAL DIGNITY</b>	<b>Order #</b>	<b>1-201</b>
<b>New/Amends/Resc:</b>	New	<b>Page:</b>	01
<b>Approved by:</b>	Chief Ken K. Antolik	<b>Officer Signature:</b>	
<b>Effective Date:</b>	July 01, 2011		
<b>Review Date:</b>			

### 1-201 INDIVIDUAL DIGNITY

As all citizens are subject to the law, they have a right to dignified treatment. All members of the BHPD are responsible for protecting this rights.



<b>Title:</b>	<b>THE ROLE OF EMPLOYEES</b>	<b>Order #</b>	<b>1-202</b>
<b>New/Amends/Resc:</b>	New	<b>Page:</b>	01
<b>Approved by:</b>	Chief Ken K. Antolik	<b>Officer Signature:</b>	
<b>Effective Date:</b>	July 01, 2011		
<b>Review Date:</b>			

### **1-202 THE ROLE OF EMPLOYEES**

Employees are the link between the Berwyn Heights Police Department and the community; As such, they may strengthen or destroy police-community relationship which may have

taken considerable effort to develop. Employees shall attempt to make each contact between themselves and the public one which inspires confidence and demonstrates professionalism.

<b>Title:</b>	<b>INTERPERSONAL COMMUNICATIONS</b>	<b>Order #</b>	<b>1-203</b>
<b>New/Amends/Resc:</b>	New	<b>Page:</b>	01
<b>Approved by:</b>	Chief Ken K. Antolik	<b>Officer Signature:</b>	
<b>Effective Date:</b>	July 01, 2011		
<b>Review Date:</b>			

### **1-203 INTERPERSONAL COMMUNICATIONS**

All employees should be aware of the stress generated by most contacts between those outside a police organization and those who are employed by the organization. Police personnel have to contend with the communications barrier developed because of the perception that police personnel are somehow different from other members of society. It is incumbent upon all employees of the BHPD to minimize and break down those barriers to effective communications between the police and the community in general.

One of the ways to more effective communications is that of treatment of individuals. All persons should be treated with dignity and respect. This isn't to say that in emergency situations lawful orders and commands cannot be issued. On the contrary, it is the responsibility of all employees to take a firm lead in times of crisis. Employees of the BHPD are trained and equipped for just this purpose. However, the manner in which an order or request is issued can initially determine the probability of a successful outcome.

<b>Title:</b>	<b>EQUITY OF TREATMENT</b>	<b>Order #</b>	<b>1-204</b>
<b>New/Amends/Resc:</b>	New	<b>Page:</b>	01
<b>Approved by:</b>	Chief Ken K. Antolik	<b>Officer Signature:</b>	
<b>Effective Date:</b>	July 01, 2011		
<b>Review Date:</b>			

#### **1-204 EQUITY OF TREATMENT**

All members of society are entitled to equitable treatment. This is to say, that all segment of the community will receive the same level of service and the same level of respectful treatment. The partnership of police and their community is

dependent upon the trust and sense of fair treatment experienced by all members of society. Without this trust, the likelihood of successful police work is in jeopardy.

<b>Title:</b>	<b>OPENNESS OF OPERATIONS</b>	<b>Order #</b>	<b>1-205</b>
<b>New/Amends/Resc:</b>	New	<b>Page:</b>	01
<b>Approved by:</b>	Chief Ken K. Antolik	<b>Officer Signature:</b>	
<b>Effective Date:</b>	July 01, 2011		
<b>Review Date:</b>			

#### **1-205 OPENNESS OF OPERATIONS**

The BHPD conducts its affairs in a professional manner, holding it's personnel to high standards of equitable treatment. This to say, that all segment of the community will receive the same level of service and the same level of

respectful treatment. Therefore, all matters, which are not confidential because of investigative necessity and are not held confidential because of law or regulation, will be made available for public disclosure.

<b>Title:</b>	<b>PRESS RELATIONS</b>	<b>Order #</b>	<b>1-300</b>
<b>New/Amends/Resc:</b>	New	<b>Page:</b>	01
<b>Approved by:</b>	Chief Ken K. Antolik	<b>Officer Signature:</b>	
<b>Effective Date:</b>	July 01, 2011		
<b>Review Date:</b>			

### **1-300 PRESS RELATIONS**

At the core of a free society is the ability of the general public to acquire and evaluate information concerning the events and activities of all aspects of that society. In this regard, the existence of a free press is essential. All elements of the

press must be allowed and encouraged to gather and report every aspect of the operation of the society. The operation of this Police Department is one of those aspects.

<b>Title:</b>	<b>RELEASE OF INFORMATION</b>	<b>Order #</b>	<b>1-301</b>
<b>New/Amends/Resc:</b>	New	<b>Page:</b>	01
<b>Approved by:</b>	Chief Ken K. Antolik	<b>Officer Signature:</b>	
<b>Effective Date:</b>	July 01, 2011		
<b>Review Date:</b>			

### **1-301 RELEASE OF INFORMATION**

If in the normal operation of police activities an unusual and newsworthy event should occur, the news media will be contacted. This contact will be made by first notifying a supervisor, or the Chief of Police, who will coordinate with the Public Information Officer 'PIO'. Contact will be made without

preference to any particular news gatherer. Instead, contact will be made generally with any and all significant news agencies which have made known their intentions to gather and distribute news of the Berwyn Heights community.



<b>Title:</b>	<b>NCIC / METERS SYSTEM SECURITY</b>	<b>Order #</b>	<b>1-301-A</b>
<b>New/Amends/Resc:</b>	New	<b>Page:</b>	01
<b>Approved by:</b>	Chief Ken K. Antolik	<b>Officer Signature:</b>	
<b>Effective Date:</b>	July 01, 2011		
<b>Review Date:</b>	July 2012		

**PURPOSE:**

To ensure that the BHPD usage of the Federal Bureau of Investigation (FBI) National Crime Information Center (NCIC) / METERS / MDT / DASHBORD is in accordance with the NCIC Security Policy.

**POLICY:**

The FBI's NCIC Security Policy requires that each criminal justice agency authorized to receive NCIC information must have appropriate written standards for discipline of NCIC violators. The BHPD will create, use, maintain, store, preserve, and dispose of information retrieved from the FBI's NCIC and the National Law Enforcement Telecommunications System (NLETS) in accordance with the NCIC Security Policy.

**DEFINITIONS:**

Criminal Justice Information System (CJIS) - a dedicated statewide network that provides instant access to criminal justice information such as criminal background information, driver license and motor vehicle registration data, as well as other data. This network is interfaced with the NCIC network that provides nationally indexed criminal and "hot" files. The CJIS is also interfaced with the NLETS, which links local, state and federal agencies together for the purpose of exchanging criminal justice information interstate.

**1-301-A NCIC / METERS SYSTEM SECURITY**

The National Crime Information Center NCIC is CONFIDENTIAL. Any information obtained from MERERS/NCIC is strictly confidential and no employees within the BHPD will disseminated information obtained / received from the said aforementioned. Any and all documentation in the form of hard copies shall be destroyed by means of shredding.

There are only three [3] legitimate reasons for accessing and obtaining III information.

III information can be obtained in connection with an authorized criminal justice investigation.

III information can be used in conjunction with a background investigation for criminal justice employment.

III information Federal agencies can use the system for background investigation in connection with security clearance as define by the Security Clearance Information Act.

## MISUSE of METERS / NCIC

- A. If the BHPD Terminal Agency Coordinator becomes aware of an employee using a NCIC/METERS/DASH-BOARD/MDT terminal, equipment, or access in a manner that is not in accordance to the CJIS's policy or NCIC policy and the problem is deemed merely operator error or substandard job performance, the agency coordinator 'AC' will contact the employee and advise him/her of the problem and provide additional training to correct the issue.
- B. If the above step does not rectify the problem, or the problem is deemed to be greater than mere operator error or substandard job performance, the AC will submit a report to the Investigative Services Section. At this time, the AC will suspend the employee's NCIC access until the Investigative Services Section conducts an investigation.
1. If the investigation does not substantiate that the employee was in violation of CJIS/BHPD Policy or NCIC Policy, the Investigative Services Section will contact the AC / Chief of Police requesting to reinstate the employee's NCIC/METERS/MDT/DASH-BOARD terminal access.

2. If the investigation substantiates that the employee was in violation of CJIS/BHPD Policy or NCIC Policy, disciplinary action may be taken against the employee. The AC / Chief of Police will deny NCIC/METERS/MDT/DASH-BOARD terminal access to the employee until directed by the Investigative Services Section to change this status.
3. If the Investigative Services Section determines that an employee is using the NCIC/METERS/MDT/DASH-BOARD terminal, equipment, or equipment access in a manner not in accordance with the NCIC/METERS/MDT/DASH-BOARD policy or NCIC policy, and there is evidence that the employee is performing this action as a result of intentional misconduct that could be in violation of state or federal statute, the Investigative Services Section will submit a report to the AC / Chief of Police for review. If the misconduct is deemed to be criminal, the Investigative Services Section will report the behavior of criminal nature to the appropriate Assistant's State Attorney for determining the appropriate action.

<b>Title:</b>	<b>Media Protection</b>	<b>Order #</b>	<b>1-301[b]</b>
<b>New/Amends/Resc:</b>	New Amended	<b>Page:</b>	01 of 03
<b>Approved by:</b>	Chief Ken K. Antolik	<b>Officer Signature:</b>	
<b>Effective Date:</b>	July 01, 2015		
<b>Review Date:</b>			

### 1. Purpose

The intent of the Media Protection Policy is to ensure the protection of the Criminal Justice Information System (CJIS) until such time as the information is either released to the public via authorized dissemination (e.g. within a court system or when presented in crime reports data), or is purged or destroyed in accordance with applicable record retention rules. The local policy may augment, or increase the standards, but shall not detract from the CJIS Security Policy standards.

### 2. Scope

The scope of this policy applies to any electronic or physical media containing any and all Criminal Justice Information System (CJIS) while being stored, accessed or physically moved from a secure location from the Berwyn Heights Police Department. This policy applies to any authorized person who accesses, stores, and / or transports electronic or physical media. Transporting CJIS outside the agency's assigned physically secure area must be monitored and controlled.

Authorized BHPD personnel shall protect and control electronic and physical CJIS while at rest and in transit. The BHPD will take appropriate safeguards for protecting CJIS to limit potential mishandling or loss while being stored, accessed, or transported. Any inadvertent or inappropriate CJIS disclosure and/or use will be reported to the BHPD TAC Officer. Procedures shall be defined for securely handling, transporting and storing media.

### 3. Media Storage and Access

Controls shall be in place to protect electronic and physical media containing CJIS while at rest, stored, or actively being accessed. "Electronic media" includes memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card. "Physical media" includes printed documents and imagery that contain CJIS.

To protect CJIS, the BHPD personnel shall:

1. Securely store electronic and physical media within a physically secure or controlled area. A secured area includes a locked drawer, cabinet, or room.

2. Restrict access to electronic and physical media to authorized individuals.

3. Ensure that only authorized users remove printed or digital media from the CJIS.

4. Physically protect CJIS until media end of life. End of life CJIS is destroyed or sanitized using approved equipment, techniques and procedures. (See *Media Sanitization Destruction Policy*)

5. Not use personally owned information system to access, process, store, or transmit CJIS unless the BHPD has established and documented the specific terms and conditions for personally owned information system usage. (See *Personally Owned Device Policy, if allowed*)

6. Not utilize publicly accessible computers to access, process, store, or transmit CJIS. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

7. Store all hardcopy CJIS printouts maintained by the BHPD in a secure area accessible to only those employees whose job function requires them to handle such documents.

8. Safeguard all CJIS by the BHPD against possible misuse by complying with the Physical Protection Policy, Personally Owned Device Policy, and Disciplinary Policy.

9. Take appropriate action when in possession of CJIS while not in a secure area:

- a. CJIS must not leave the employee's immediate control. CJIS printouts cannot be left unsupervised while physical controls are not in place.

- b. Precautions must be taken to obscure CJIS from public view, such as by means of an opaque file folder or envelope for hard copy printouts. For electronic devices like laptops, use session lock use and /or privacy screens. CJIS shall not be left in plain public view. When CJIS is electronically transmitted outside the



boundary of the physically secure location, the data shall be immediately protected using encryption.

10. Lock or log off computer when not in immediate vicinity of work area to protect CJIS. Not all personnel have same CJIS access permissions and need to keep CJIS protected on a need-to-know basis.

11. Establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of CJIS. (See *Physical Protection Policy*)

#### **4.0 Media Transport**

Controls shall be in place to protect electronic and physical media containing CJIS while in transport (physically moved from one location to another) to prevent inadvertent or inappropriate disclosure and use. "Electronic media" means electronic storage media including memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card. Dissemination to another agency is authorized if:

1. The other agency is an Authorized Recipient of such information and is being serviced by the accessing agency, or
2. The other agency is performing personnel and appointment functions for criminal justice employment applicants.

The BHPD personnel shall:

1. Protect and control electronic and physical media during transport outside of controlled areas.
2. Restrict the pickup, receipt, transfer and delivery of such media to authorized personnel.

The BHPD personnel will control, protect, and secure electronic and physical media during transport from public disclosure by:

1. Use of privacy statements in electronic and paper documents.
2. Limiting the collection, disclosure, sharing and use of CJIS.
3. Following the least privilege and role based rules for allowing access. Limit access to CJIS to only those people or roles that require access.
4. Securing hand carried confidential electronic and paper documents by:
  - a. Storing CJIS in a locked briefcase or lockbox.
  - b. Only viewing or accessing the CJI electronically or document printouts in a physically secure location by authorized personnel.
  - c. For hard copy printouts or CJIS documents:

i. Package hard copy printouts in such a way as to not have any CJIS information viewable.

ii. That are mailed or shipped, agency must document procedures and only release to authorized individuals. DO NOT MARK THE PACKAGE TO BE MAILED CONFIDENTIAL. Packages containing CJIS material are to be sent by method(s) that provide for complete shipment tracking and history, and signature confirmation of delivery.

5. Not taking CJIS home or when traveling unless authorized by BHPD TAC officer or the Chief of Police. When disposing confidential documents, use a cross-cut shredder.

#### **5.0 Electronic Media Sanitization and Disposal**

The agency shall sanitize, that is, overwrite at least three times or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. Inoperable electronic media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel. Physical media shall be securely disposed of when no longer required, using formal procedures. For end of life media policy, refer to "Media Sanitization Destruction Policy".

#### **6.0 Breach Notification and Incident Reporting**

The agency shall promptly report incident information to appropriate authorities. Information security events and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken. Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/Commander's Log with assigned CCN numbers.

#### **7.0 Roles and Responsibilities**

If CJIS is improperly disclosed, lost, or reported as not received, the following procedures must be immediately followed:

1. BHPD personnel shall notify his/her supervisor or TAC officer, and an incident-report form must be completed and submitted within 24 hours of discovery of the incident. The submitted report is to contain a detailed account of the incident, events leading to the incident, and steps taken/to be taken in response to the incident.
2. The supervisor will communicate the situation to the TAC officer to notify of the loss or disclosure of CJI records.
3. The TAC officer will ensure the (CJIS System Agency Information Security Officer) is promptly informed of security incidents.
4. The TAC officer will:

a. Establish a security incident response and reporting procedure to discover, investigate, document, and report to the Chief of Police, the affected criminal justice agency, and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJIS.

b. Collect and disseminate all incident-related information received from the Department of Justice (DOJ), FBI CJIS Division, and other entities to the appropriate local law enforcement within their area.

#### **8.0 Penalties**

Violation of any of the requirements in this policy by any authorized personnel will result in suitable disciplinary action, up to and including loss of access privileges, civil and criminal prosecution and / or termination.

Other Related Resources:

- Media Sanitization and Destruction Policy (Required)
- Physical Protection Policy (Required)
- Personally Owned Device Policy (if allowed) (Required)

<b>Title:</b>	<b>Media Sanitization and Destruction</b>	<b>Order #</b>	<b>1-500[c]</b>
<b>New / Amends / Resc:</b>	New Amended	<b>Page:</b>	01 of 03
<b>Approved by:</b>	Chief Ken K. Antolik	<b>Officer Signature:</b>	
<b>Effective Date:</b>	July 01, 2015		
<b>Review Date:</b>			

## 1. Purpose

The purpose of this policy is to protect the Berwyn Heights Police Department from unauthorized disclosure. This policy defines the requirements for ensuring Agency's Data are permanently removed from media before disposal or reuse, a process called "media sanitization," and properly disposing of media. The reuse, recycling, or disposal of computers and other technologies that can store data pose a significant risk since data can easily be recovered with readily available tools - even data from files that were deleted long ago or a hard drive that was reformatted. Failure to properly purge data in these circumstances may result in unauthorized access to the BHPD Data, breach of software license agreements, and/or violation of state and federal data security and privacy laws.

## 2. Scope

This policy applies to all BHPD employees.

## 3. Effective Date

This policy became effective on July 01, 2015.

## 4. Authority

The BHPD *Media Sanitization and Disposal Policy* requires policies and procedures for the sanitization of all media including hard copy and electronic.

## 5. Policy

To prevent unauthorized disclosure of classified and or unclassified Data, media leaving control of the responsible department and destined for reuse or disposal must have all agency's Data purged in a manner that renders the data unrecoverable.

Media that will be reused within the department should likewise have all BHPD Data purged to prevent unauthorized disclosure.

Media containing BHPD Data authorized by the Chief of Police for transfer to individuals are exempt.

## 6. Definitions

- A. *Affiliated Organization* - any organization associated with the BHPD that uses BHPD information technology resources to create, access, store or manage BHPD Data to perform their business functions.
- B. *Confidential Data* - Highly sensitive BHPD Data intended for limited, specific use by a workgroup, department, or group of individuals with a legitimate need-to-know.
- C. *DeGaussing* - demagnetizing magnetic storage media like tape or a hard disk drive to render it permanently unusable. Since the media typically can no longer be used after degaussing, it should only be used to purge data from media that will be discarded.
- D. *Disintegration* - A physically destructive method of sanitizing data; the act of separating into component parts.



- E. *HIPAA* - Health Insurance Portability and Accountability Act of 1996 that among other things established standards for the security and privacy of human health-related information.
- F. *Incineration* - A physically destructive method of sanitizing media; the act of burning completely to ashes.
- G. *Internal Data* - BHPD Data intended for internal use only with access restricted to a specific workgroup, department, group of individuals, or affiliates with a legitimate need.
- H. *Media* - material on which data are or may be recorded, such as magnetic disks or tapes, solid state devices like USB flash drives, optical discs like CDs and DVDs, or paper-based products.
- I. *Media sanitization* - the process of removing data from storage media such that there is reasonable assurance that the data may not be retrieved and reconstructed.
- J. *Pulverization* - A physically destructive method of sanitizing media; the act of grinding to a powder or dust.
- K. *Purging* - a media sanitization process that removes all data and any remnant of the data so thoroughly that the effort required to recover the data, even with sophisticated tools in a laboratory setting (i.e., a "laboratory attack"), exceeds the value to the attacker. A common method of purging data is to overwrite it with random data in three or more passes.

Likewise, it is often most cost effective to physically destroy the media rather than expend the effort to properly purge data. However, if physical destruction is contracted to a third party outside the BHPD, all Agency's Data must be purged from the media before giving it to the third party.

Specific instructions for different types of media and regulations follow.

*A. Electronic Storage Media (hard disk drives in computers, external hard drives, USB flash drives, magnetic tapes, etc.)*

1. If purging is done by overwriting the data, the *entire media/device* must be overwritten with a minimum of three passes.
2. Equipment that can store BHPD Data, such as desktop and laptop computers or external hard drives, and is permanently leaving the control of the agency should have all data storage devices removed before disposition. If the equipment leaving BHPD control must retain the data storage devices, all BHPD Data must be properly purged.
3. The only acceptable methods for physically destroying a hard drive are shredding, pulverizing, disintegration, or incineration.
4. Degaussing is an acceptable method of purging data from magnetic media. Be aware that this normally renders the media unusable.

*B. Paper-Based Media*

1. Any paper-based or other hard copy media containing confidential BHPD Data must be shredded with a cross-cut shredder before disposal or transferred to an authorized third party contracted by the BHPD for secure disposition of documents. The maximum particle size for paper-based media containing confidential data should be 1x5 mm (1/32"x1/5"). Media containing internal data should likewise be shredded with a cross-cut shredder if disclosure of the information contained therein might adversely impact the institution, an affiliated organization, or an individual. The maximum particle size for media containing internal data is 2x15 mm (1/16"x3/5").
2. Incineration by methods compliant with all relevant health, safety, and environmental laws

## 7. Roles and Responsibilities

The BHPD is responsible for ensuring that Agency's Data are properly removed or destroyed from media before it leaves the control of the department for reuse or disposal.

## 8. Implementation Procedures

While the primary purpose of this policy is to protect non-public Agency's Data (e.g., data classified either internal or confidential), it is often very difficult to separate these classifications from public or personal data on the media, or determine conclusively that remnants of non-public data are not recoverable. Therefore, it is often most expedient and cost effective to purge all BHPD Data from the media before reuse or disposal rather than try to selectively sanitize the sensitive data.

and regulations is an acceptable method for disposal of paper-based media.

*C. Optical Media (e.g., CDs and DVDs)*

Optical media containing internal or confidential BHPD Data must be physically destroyed before disposal. An appropriate method of physical destruction is shredding with a cross-cut shredder.

*D. Smartphones, Personal Digital Assistants (PDAs), and other handheld devices*

Mobile devices like Smartphones (e.g., Blackberry or Treo), PDAs, MP3 players, and even regular cell phones store information and often contain personal or other sensitive information. Any BHPD Data must be purged from these devices before reuse or disposal, like any other storage media. It is also advisable to purge all other data from the device before reuse or disposal to protect your personal information.



<b>Title:</b>	<b>Media Physical Protection</b>	<b>Order #</b>	<b>1-500[d]</b>
<b>New/Amends/Resc:</b>	New Amended	<b>Page:</b>	01 of 06
<b>Approved by:</b>	Chief Ken K. Antolik	<b>Officer Signature:</b>	
<b>Effective Date:</b>	July 01, 2015		
<b>Review Date:</b>			

### 1. Purpose:

The purpose of this policy is to provide guidance for agency personnel, support personnel, and private contractors/vendors for the physical, logical, and electronic protection of Criminal Justice Information System (CJIS). All physical, logical, and electronic access must be properly documented, authorized and controlled on devices that store, process, or transmit unencrypted CJIS. This Physical Protection Policy focuses on the appropriate access control methods needed to protect the full lifecycle of CJIS from insider and outsider threats.

### 2. Physically Secure Location:

A physically secure location is a facility or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect the CJIS and associated information systems. The perimeter of the physically secure location shall be prominently posted and separated from non-secure locations by physical controls. Security perimeters shall be defined, controlled, and secured. Restricted non-public areas in the BHPD shall be identified with a sign at the entrance.

### 3. Visitors Access:

A visitor is defined as a person who visits the BHPD facility on a temporary basis who is not employed by the BHPD and has no unescorted access to the

physically secure location within the BHPD where CJIS and associated information systems are located.

Visitors shall:

1. Check in before entering a physically secure location by:

- a. Provide a form of identification used to authenticate visitor.

- b. In the event if the BHPD issues visitor badges, the visitor badge shall be worn on approved visitor's outer clothing and collected by the agency at the end of the visit.

2. Be accompanied by a BHPD escort at all times to include delivery or service personnel. An escort is defined as authorized personnel who accompany a visitor at all times while within a physically secure location to ensure the protection and integrity of the physically secure location and any CJIS therein. The use of cameras or other electronic means used to monitor a physically secure location does not constitute an escort.

3. Show BHPD personnel a valid form of photo identification.

4. Follow BHPD policy for authorized unescorted access.



a. Noncriminal Justice Agency (NCJA) like city or county IT who require frequent unescorted access to restricted area(s) will be required to establish a **Management Control Agreement** between the BHPD and NCJA. Each NCJA employee with CJIS access will appropriately have state and national fingerprint-based record background check prior to this restricted area access being granted.

b. Private contractors/vendors who requires frequent unescorted access to restricted area(s) will be required to establish a CJIS **Security Addendum** between the BHPD and each private contractor personnel. Each private contractor personnel will appropriately have state and national fingerprint-based record background check prior to this restricted area access being granted.

5. Not be allowed to view screen information mitigating shoulder surfing.

6. Individuals not having any legitimate business in a restricted area shall be courteously escorted to a public area of the facility. Strangers in physically secure areas without an escort should be challenged. If resistance or behavior of a threatening or suspicious nature is encountered, sworn personnel shall be notified or call 911.

7. Not be allowed to sponsor another visitor.

8. Not enter into a secure area with electronic devices unless approved by the BHPD Local Area Security Officer (LASO), or TAC to include cameras and mobile devices. Photographs are not allowed without permission of the BHPD assigned personnel.

9. All requests by groups for tours of the BHPD facility will be referred to the proper agency point of contact for scheduling. In most cases, these groups will be handled by a single form, to be signed by a designated group leader or representative. Remaining visitor rules apply for each visitor within the group. The group leader will provide a list of names to front desk personnel for instances of emergency

evacuation and accountability of each visitor while on agency premises.

#### **4. Authorized Physical Access:**

Only authorized personnel will have access to physically secure non-public locations. The BHPD will maintain and keep current a list of authorized personnel. All physical access points into the agency's secure areas will be authorized before granting access. The agency will implement access controls and monitoring of physically secure areas for protecting all transmission and display mediums of CJIS. Authorized personnel will take necessary steps to prevent and protect the agency from physical, logical and electronic breaches.

All personnel with CJIS physical and logical access must:

1. Meet the minimum personnel screening requirements prior to CJIS access.

a. To verify identification, a state of residency and national fingerprint-based record checks shall be conducted within 30 days of assignment for all personnel who have direct access to CJIS and those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJIS.

b. Support personnel, private contractors/vendors, and custodial workers with access to physically secure locations or controlled areas (during CJIS processing) shall be subject to a state and national fingerprint-based record check unless these individuals are escorted by authorized personnel at all times.

c. Prior to granting access to CJIS, the BHPD on whose behalf the contractor is retained shall verify identification via a state of residency and national fingerprint-based record check.

d. Refer to the CJIS Security Policy for handling cases of felony convictions, criminal records, arrest histories, etc.

2. Complete security awareness training.

a. All authorized BHPD, Noncriminal Justice Agencies (NCJA) like city or county IT and private contractor/vendor personnel will receive security awareness training within six months of being granted duties that require CJIS access and every two years thereafter.

b. Security awareness training will cover areas specified in the CJIS Security Policy at a minimum.

3. Be aware of who is in their secure area before accessing confidential data.

a. Take appropriate action to protect all confidential data.

b. Protect all terminal monitors with viewable CJIS displayed on monitor and not allow viewing by the public or escorted visitors.

4. Properly protect and not share any individually issued keys, proximity cards, computer account passwords, etc.

a. Report loss of issued keys, proximity cards, etc to authorized supervisor personnel, or the Chief of Police.

b. If the loss occurs after normal business hours, or on weekends or holidays, personnel are to call the BHPD POC to have authorized credentials like a proximity card de-activated and/or door locks possibly rekeyed.

c. Safeguard and not share passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), and all other facility and computer systems security access procedures.

5. Properly protect from viruses, worms, Trojan horses, and other malicious code.

6. Web usage—allowed versus prohibited; monitoring of user activity.

7. Do not use personally owned devices on the BHPD computers with CJIS access.

8. Use of electronic media is allowed only by authorized BHPD personnel. Controls shall be in place to protect electronic media and printouts containing CJIS while in transport. When CJIS is physically moved from a secure location to a non-secure location, appropriate controls will prevent data compromise and/or unauthorized access.

9. Encrypt emails when electronic mail is allowed to transmit CJIS-related data as such in the case of Information Exchange Agreements.

a. Agency Discretion for allowance of CJIS via email.

b. If CJIS is transmitted by email, the email must be encrypted end-to-end and email recipient must be authorized to receive and view CJIS.

10. Report any physical security incidents to the BHPD's supervisor or the Chief of Police to include facility access violations, loss of laptops, Blackberries, thumb drives, CDs/DVDs and printouts containing CJIS.

11. Properly release hard copy printouts of CJIS only to authorized vetted and authorized personnel in a secure envelope and shred or burn hard copy printouts when no longer needed. Information should be shared on a "need to know" basis. (See Media Sanitization and Destruction Policy 1-600[c])

12. Ensure data centers with CJIS are physically and logically secure.

13. Keep appropriate BHPD security personnel informed when CJIS access is no longer needed. In the event of ended employment, the individual must surrender all property and access managed by the local agency, state and/or federal agencies.

14. Not use food or drink around information technology equipment.

15. Know which door to use for proper entry and exit of the BHPD and only use marked alarmed fire exits in emergency situations.

16. Ensure the perimeter security door securely locks after entry or departure. Do not leave any perimeter door propped open and take measures to prevent piggybacking entries.

## **5. Roles and Responsibilities:**

### **5.1 Terminal Agency Coordinator (TAC)**

The TAC serves as the point-of-contact at the BHPD for matters relating to CJIS information access. The TAC administers CJIS systems programs within the agency and oversees the agency's compliance with FBI and MI CJIS systems policies/addenda.

1. Identify who is using the approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
2. Identify and document how the equipment is connected to the state system.
3. Ensure that personnel security screening procedures are being followed as stated in this policy.
4. Ensure the approved and appropriate security measures are in place and working as expected.
5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

### **5.2 Agency Coordinator (AC)**

An AC is a staff member of the Contracting Government Agency (CGA) who manages the agreement between the private contractor(s)/vendor(s) and the BHPD. A CGA is a government agency, whether a Criminal Justice Agency (CJA) or a NCJA, that enters into an agreement with a private contractor/vendor subject to the CJIS Security Addendum. The AC shall be responsible for the supervision and integrity of the system, training and continuing education of private contractor/vendor employees and operators,

scheduling of initial training and testing, and certification testing and all required reports by LEIN/NCIC.

### **5.5 Information Technology Support**

In coordination with above roles, all vetted IT support staff will protect CJIS from compromise at the BHPD by performing the following:

1. Protect information subject to confidentiality concerns – in systems, archived, on backup media, and until destroyed. Know where CJIS is stored, printed, copied, transmitted and planned end of life. CJIS is stored on laptops, mobile data terminals (MDTs), computers, servers, tape backups, CDs, DVDs, thumb drives, and internet connections as authorized by the BHPD
2. Be knowledgeable of required BHPD technical requirements and policies taking appropriate preventative measures and corrective actions to protect CJIS at rest, in transit and at the end of life.
3. Take appropriate action to ensure maximum uptime of CJIS and expedited backup restores by using agency approved best practices for power backup and data backup means such as generators, backup universal power supplies on CJIS-based terminals, servers, switches, etc.
4. Properly protect the BHPD's CJIS system(s) from viruses, worms, Trojan horses, and other malicious code (real-time scanning and ensure updated definitions).
  - a. Install and update antivirus on computers, laptops, MDTs, servers, etc.
  - b. Scan any outside non-agency owned CDs, DVDs, thumb drives, etc., for viruses, if the BHPD allows the use of personally owned devices. (See Personally Owned Device Policy)
5. Data backup and storage – centralized or decentralized approach.

a. Perform data backups and take appropriate measures to protect all stored CJIS.

b. Ensure only authorized vetted personnel transport off-site tape backups or any other media that store CJIS that is removed from physically secured location.

c. Ensure any media released from the [agency name] is properly sanitized / destroyed. (See Media Sanitization and Destruction Policy)

6. Timely application of system patches—part of configuration management.

a. The agency shall identify applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws.

b. When applicable, see the BHPD Patch Management Policy.

7. Access control measures

a. Address least privilege and separation of duties.

b. Enable event logging of:

i. Successful and unsuccessful system log-on attempts.

ii. Successful and unsuccessful attempts to access, create, write, delete or change permission on a user account, file, directory or other system resource.

iii. Successful and unsuccessful attempts to change account passwords.

iv. Successful and unsuccessful actions by privileged accounts.

v. Successful and unsuccessful attempts for users to access, modify, or destroy the audit log file.

c. Prevent authorized users from utilizing publicly accessible computers to access, process, store, or transmit CJIS. Publicly accessible computers include

but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

8. Account Management in coordination with TAC

a. Agencies shall ensure that all user IDs belong to currently authorized users.

b. Keep login access current, updated and monitored. Remove or disable terminated or transferred or associated accounts.

c. Authenticate verified users as uniquely identified.

d. Prevent multiple concurrent active sessions for one user identification, for those applications accessing CJIS, unless the agency grants authority based upon operational business needs.

e. Not use shared generic or default administrative user accounts or passwords for any device used with CJIS.

f. Passwords

i. Be a minimum length of eight (8) characters on all systems.

ii. Not be a dictionary word or proper name.

iii. Not be the same as the User ID.

iv. Expire within a maximum of 90 calendar days.

v. Not be identical to the previous ten (10) passwords.

vi. Not be transmitted in the clear or plaintext outside the secure location.

vii. Not be displayed when entered.

viii. Ensure passwords are only reset for authorized user.

9. Network infrastructure protection measures.

a. Take action to protect CJIS-related data from unauthorized public access.



b. Control access, monitor, enabling and updating configurations of boundary protection firewalls.

c. Enable and update personal firewall on mobile devices as needed.

d. Ensure confidential electronic data is only transmitted on secure network channels using encryption and \*advanced authentication when leaving a physically secure location. No confidential data should be transmitted in clear text. \*Note: a police vehicle shall be considered a physically secure location.

e. Ensure any electronic media that is removed from a physically secured location is encrypted in transit by a person or network.

f. Not use default accounts on network equipment that passes CJIS like switches, routers, firewalls.

g. Make sure law enforcement networks with CJIS shall be on their own network accessible by authorized personnel who have been vetted by the BHPD. Utilize Virtual Local Area Network (VLAN) technology to segment CJIS traffic from other noncriminal justice agency traffic to include other city and/or county agencies using same wide area network.

10. Communicate and keep the BHPD informed of all scheduled and unscheduled network and computer downtimes, all security incidents and misuse. The ultimate information technology management control belongs to BHPD.

#### 5.6 Visitor Access/Security

Administration of the Visitor Check-In / Check-Out procedure is the responsibility of identified individuals in each facility.

Prior to visitor gaining access to physically secure area:

1. The visitor will be screened by the BHPD personnel for weapons. No weapons are allowed in the agency

except when carried by authorized personnel as deemed authorized by the BHPD.

2. The visitor will be screened for electronic devices. No personal electronic devices are allowed in any agency facility except when carried by authorized personnel as deemed authorized by the BHPD.

3. Escort personnel will acknowledge being responsible for properly evacuating visitor in cases of emergency. Escort personnel will know appropriate evacuation routes and procedures.

4. Escort personnel will validate visitor is not leaving agency with any agency owned equipment or sensitive data prior to visitor departure.

All BHPD personnel and supporting entities are responsible to report any unauthorized physical, logical, and electronic access to the NHPD officials. For BHPD, the point of contacts to report any non-secure access is:

Name: Chief Kenneth K. Antolik |Phone: 301-474-6554 (240) 508-9940

email: Chief@BerwynHeightsPD.com

TAC Name: Scott Krouse | Phone: 301-474-6554

TAC email: SKrouse@BerwynHeightsPD.com

#### 6. Penalties:

Violation of any of the requirements in this policy by any authorized personnel will result in suitable disciplinary action, up to and including loss of access privileges, civil and criminal prosecution and / or termination.

Violation of any of the requirements in this policy by any visitor can result in similar disciplinary action against the sponsoring employee, and can also result in termination of services with any associated consulting organization or prosecution in the case of criminal activity.

<b>Title:</b>	<b>PRESS ACCESS TO SCENE</b>	<b>Order #</b>	<b>1-302</b>
<b>New/Amends/Resc:</b>	New	<b>Page:</b>	01
<b>Approved by:</b>	Chief Ken K. Antolik	<b>Officer Signature:</b>	
<b>Effective Date:</b>	July 01, 2011		
<b>Review Date:</b>			

### **1-302 PRESS ACCESS TO SCENE**

Officers in charge of scene may permit press access inside police line for news gathering purpose. The officer in charge of the scene should evaluate the danger to the press, the possible contamination of the scene, the need to protect sensitive evidence and information and any interference which might occur with an ongoing investigation or incident. If these considerations can be resolve, the officer in charge may permit controlled access to the degree possible under the instant circumstances. The scope of the allowed press access should be clearly defined for all press persons allowed across police lines. Those persons should then be continuously escorted or limited to a particular area which

can be controlled by the officer in charge. The identity of each press person should be known to the officer in charge or should be proven by press credentials before entry is allowed. Free lance journalist will be treated as private citizens. Press persons should be denied access, or removed from a previously granted access, at any time their presence jeopardizes a legitimate police purpose. In making decisions concerning the access of press persons at scene, officer in charge should be aware that these persons have the same statutory responsibilities and are subject to the same laws and rules as are any other citizen.

<b>Title:</b>	<b>POLICE REQUEST TO WITHHOLD INFORMATION</b>	<b>Order #</b>	<b>1-303</b>
<b>New/Amends/Resc:</b>	New	<b>Page:</b>	01
<b>Approved by:</b>	Chief Ken K. Antolik	<b>Officer Signature:</b>	
<b>Effective Date:</b>	July 01, 2011		
<b>Review Date:</b>			

### **1-303 POLICE REQUEST TO WITHHOLD INFORMATION**

News gathering representative may photograph or report anything they observe where they are legally present at an incident scene. Where publication of such coverage would interfere with an official investigation or place a victim, suspect or others in jeopardy, the withholding of publication is dependant upon a cooperative press, not upon censorship by

the police agency. Under such circumstances, officer should advise the media representative s or their superior of the possible consequences of publication. However, officers may not interfere with news gathering activities as long as the performance of that action remains legal.

<b>Title:</b>	<b>INDIVIDUAL PRESS STATEMENTS</b>	<b>Order #</b>	<b>I-304</b>
<b>New/Amends/Resc:</b>	<b>New</b>	<b>Page:</b>	<b>01</b>
<b>Approved by:</b>	<b>Chief Ken K. Antolik</b>	<b>Officer Signature:</b>	
<b>Effective Date:</b>	<b>July 01, 2011</b>		
<b>Review Date:</b>			

### **I-304 INDIVIDUAL PRESS STATEMENTS**

No employee of the BHPD, except the Chief of Police, or his designee may make a statement to the press or news gathering media concerning the operations or administration of the agency; and no statement may be made concerning the employee's personal role in any operation or administrative activity of the agency without permission of a supervisor or the Chief of Police. His policy is made to prevent individual employees from mistakenly representing the Agency without first having the benefit of all facts and information which may effect such representation. In this way, statements made by Agency personnel will be more likely accurately represent Agency policies and provide the media's representatives with more complete information. It is better to do it right the first time then to try to correct erroneous or harmful information which has already been made public.

If there is a known possibility of civil action against an employee or the Agency concerning an event, statements will not be made without the authorization of the Chief of Police. Individual employees will refrain from making statements concerning their personal opinion of the truthfulness of any statements made by any victim or witness associated with an investigation.

<b>Title:</b>	<b>PRESS RELEASES</b>	<b>Order #</b>	<b>1-305</b>
<b>New/Amends/Resc:</b>	<b>New</b>	<b>Page:</b>	<b>01</b>
<b>Approved by:</b>	<b>Chief Ken K. Antolik</b>	<b>Officer Signature:</b>	
<b>Effective Date:</b>	<b>July 01, 2011</b>		
<b>Review Date:</b>			

# 1-305 PRESS RELEASES

Press releases will be made concerning the following:

- Felony criminal investigations
- Serious or unusual misdemeanor criminal investigations
- All arrests
- All motor vehicle accidents with injuries
- All fatal motor vehicles accidents
- All serious hit and run accidents
- Arrests or citation issued for alcohol violations [names of juveniles to be withheld]
- Incidents occurring within public schools [names of juveniles to be withheld]
- Vehicle thefts, including make/model/color/year and registration number of stolen vehicle.

Information which will not be included in the press releases and which will be kept confidential shall include:

- The name of witnesses or victims of crimes
- The names of accused child abusers when identifying the accused would likely identify the victim(s)
- The names of deceased person prior to notification of the next of kin
- Criminal history information
- Information concerning admissions or confessions of accused persons
- Specific dollar amounts of cash or property involve (except that an indication of whether the amount is over or under \$1,000.00, and
- Any information, which in the opinion of the investigating officer could impede the ongoing criminal investigation or prosecution.



<b>Title:</b>	<b>PRESS RELEASE PROCEDURE</b>	<b>Order #</b>	<b>1-306</b>
<b>New/Amends/Resc:</b>	New	<b>Page:</b>	01
<b>Approved by:</b>	Chief Ken K. Antolik	<b>Officer Signature:</b>	
<b>Effective Date:</b>	July 01, 2011		
<b>Review Date:</b>			

### **1-306 PRESS RELEASE PROCEDURE**

Press release will be completed at the end of each week and submitted to the Mayor and Council. In addition the press release can be found uploaded by the BHPD webmaster at the end of each week. The media or any citizen can view the press release information which is located at the [www.BerwynHeightsPD.com](http://www.BerwynHeightsPD.com). When media representative

request further information regarding a press release or incident, they will be referred to a supervisor or the PIO for further questions. Members of the media should not be referred to the investigating officer for further questions without supervisory approval.

<b>Title</b>	<b>REQUEST BY CITIZENS FOR RESTRICTED RELEASE OF INFORMATION</b>	<b>Order #</b>	<b>1-307</b>
<b>New/Amends/Resc:</b>	New	<b>Page:</b>	01
<b>Approved by:</b>	Chief Ken K. Antolik	<b>Officer Signature:</b>	
<b>Effective Date:</b>	July 01, 2011		
<b>Review Date:</b>			

### **1-307 REQUESTS BY CITIZENS FOR RESTRICTED RELEASE OF INFORMATION**

Whenever a citizens requests that information concerning a particular incident not be release to the media, employees shall explain that police reports are generally considered public information, and therefore, accessible to the media.

Employees shall explain that such a request will be noted in the official report, but that the media will make the decision whether or not to publish publicly available information.

<b>Title:</b>	<b>PUBLIC INFORMATION</b>	<b>Order #</b>	<b>1-400</b>
<b>New/Amends/Resc:</b>	New	<b>Page:</b>	01
<b>Approved by:</b>	Chief Ken K. Antolik	<b>Officer Signature:</b>	
<b>Effective Date:</b>	July 01, 2011		
<b>Review Date:</b>			

#### **1-400 PUBLIC INFORMATION**

It is policy of the BHPD to comply with all legitimate requests for information concerning its actions and operations. Because of the technical nature of those requests, all of those

requests, which are not specifically covered elsewhere in this manual, will be referred to the Chief of Police.

<b>Title</b>	<b>FEATURE ARTICLES OF PROGRAM OPERATIONS</b>	<b>Order #</b>	<b>1-401</b>
<b>New/Amends/Resc:</b>	New	<b>Page:</b>	01
<b>Approved by:</b>	Chief Ken K. Antolik	<b>Officer Signature:</b>	
<b>Effective Date:</b>	July 01, 2011		
<b>Review Date:</b>			

#### **1-401 FEATURE ARTICLES OF PROGRAM OPERATIONS**

Requests for Agency participation in feature articles and programs and the photographing of BHPD vehicles, clothing, badges, insignia, equipment and personnel, as well as the police facility, will be limited to the scope of approval obtained by the media company from the Chief of Police for such article or program. Employees participating in the preparation of such article or programs should ascertain the

scope of the approval and should be careful not to exceed those limits. In any event, employees should exercise care and discretion to avoid making statements or conveying information which, if later quoted, would create a misunderstanding or compromise the effectiveness of the Agency.

<b>Title:</b>	<b>LABOR RELATIONS</b>	<b>Order #</b>	<b>I-500</b>
<b>New/Amends/Resc:</b>	New	<b>Page:</b>	01
<b>Approved by:</b>	Chief Ken K. Antolik	<b>Officer Signature:</b>	
<b>Effective Date:</b>	July 01, 2011		
<b>Review Date:</b>			

### **I-500    LABOR RELATIONS**

It is policy of the BHPD to be an impartial observer in labor dispute. The Agency's only role is that of ensuring order and the obedience of rule of law. When members of this Agency are called to or otherwise have the occasion to be at the scene of a labor dispute they will conduct their activities to prevent violations of the law and to protect all parties from lawless acts.

Officers will take action to see that free access is allowed to all persons using public roads, sidewalks and parking lots.

Those who seek to block or disrupt such access will be required to obey the law or face arrest.

Officers are not normally deployed at scene of labor disputes. However, if conditions exist which require the deployment of agency personnel in such case, a supervisor will assume control of such deployment.



<b>Title:</b>	<b>UNIFORM &amp; EQUIPMENT</b>	<b>Order #</b>	<b>1-600</b>
<b>New/Amends/Resc:</b>	New	<b>Page:</b>	01
<b>Approved by:</b>	Chief Ken K. Antolik	<b>Officer Signature:</b>	
<b>Effective Date:</b>	July 01, 2011		
<b>Review Date:</b>			

## I. PURPOSE

The purpose of this policy is to set forth guidelines to standardize the uniform of this agency.

## II. POLICY

It is the policy of this agency that all personnel will present a standardized image to the public.

## III. UNIFORM REGULATIONS

All officers of the department while on duty, with the exception of officers for whom civilian attire has been authorized, shall wear the appropriate uniform. Shirts shall be buttoned their full length, except that the top button of the shirt should be left open when not wearing a tie. Partial wearing of the uniform, while in public, is strictly prohibited.

## IV. UNIFORMED OFFICERS

### A. SEASONAL CHANGE AND CLASSIFICATION OF UNIFORMS FOR SUPERVISORS.

1. CLASS "A" UNIFORM - will consist of the long sleeve gray uniform shirt, and dark navy uniform tie and department issued hat. When a long sleeve shirt is being worn, the sleeves will be extended their full length. At no time will the sleeves be rolled up on the arm.

2. *WINTER DUTY UNIFORM Class "1"* - Long sleeve gray uniform shirts 'Flying Cross-Duro Poplin' 65% Dacron Polyester 35% Cotton #35W5441, with/ without tie, dark navy blue freedom fit by 'Fechheimer' poly-wool blend pants with silver stripes #RN28562 may be worn beginning October 1<sup>st</sup>, at the discretion of the Division Commander. On and after November 1, until March 1<sup>st</sup>, the winter duty uniform shall be worn. This is the regular duty uniform for all Patrolpersons in winter. When a long sleeve shirt is being worn, the sleeves will be extended their full length. At no time will the sleeves be rolled up on the arm. (*When dealing with the public, tie must be on unless wearing a BHPD issued turtleneck.*)

3. *SUMMER DUTY UNIFORM Class "1"* - Short sleeve gray 'Flying Cross-Duro Poplin' 65% Dacron Polyester 35% Cotton #35W5441, navy blue freedom fit by 'Fechheimer' poly-wool blend pants with silver stripes #RN28562 may be worn on or after March 1<sup>st</sup>, at the discretion of the Agency's 2<sup>nd</sup> in command. On and after April 1<sup>st</sup>, until October 1<sup>st</sup>, the summer uniform shall be worn. This is the regular duty uniform for all Patrolpersons in summer.

4. *WINTER DUTY UNIFORM Class "2"* - Long sleeve gray uniform shirts Tactical 'Tru-Spec' 65% Dacron Polyester 35% Cotton #1416, without tie, and black 'Tru-Spec' #1062 Tactical pants may be worn beginning October 1<sup>st</sup>, at the discretion of the Agency's 2<sup>nd</sup> in command for



evening/midnight shift. On and after November 1, until March 1<sup>st</sup>, the winter duty uniform shall be worn. This is the regular duty uniform for all Patrolpersons in winter. When a long sleeve shirt is being worn, the sleeves will be extended their full length. At no time will the sleeves be rolled up on the arm. *(When dealing with the public, tie must be on unless wearing a BHPD issued turtleneck.)*

5. **SUMMER DUTY UNIFORM Class "2"** - Short sleeve gray Tactical 'Tru-Spec' 65% Dacron Polyester 35% Cotton #1416, and black 'Tru-Spec' #1062 Tactical pants may be worn on or after March 1<sup>st</sup>, at the discretion of the Agency's 2<sup>nd</sup> in command. On and after April 1<sup>st</sup>, until October 1<sup>st</sup>, the summer uniform shall be worn. This is the regular duty uniform for all Patrolpersons in summer.

6. A white crew neck undershirt shall be worn under the gray uniform shirt for Class "1" and black crew neck undershirt for Class "2".

a. **BATTLE DRESS UNIFORMS (BDU's)** -

The Battle Dress Uniform is not authorized as a regular duty uniform. Only officers working special assignments as directed by the Chief of Police or his designee will wear the BDU uniform. A black crew neck undershirt shall be worn under the Battle Dress Uniform shirt.

**B. SEASONAL CHANGE AND CLASSIFICATION OF UNIFORMS FOR PATROLPERSONS.**

1. **CLASS "A" UNIFORM** - will consist of the long sleeve gray, dark navy uniform tie, and department issued hat. When a long sleeve shirt is being worn, the sleeves will be extended their full length. At no time will the sleeves be rolled up on the arm.

2. **WINTER DUTY UNIFORM Class "1"** - Long sleeve gray uniform shirts 'Flying Cross-Duro Poplin' 65% Dacron Polyester 35% Cotton #35W5441, with/ without tie, dark navy blue freedom fit by 'Fechheimer' poly-wool blend pants with silver stripes #RN28562 may be worn beginning October 1<sup>st</sup>, at the discretion of the Division Commander. On and after November 1, until March 1<sup>st</sup>, the winter duty uniform shall be worn. This is the regular duty uniform for all Patrolpersons in winter. When a long sleeve shirt is being worn, the sleeves will be extended their full length. At no time will the sleeves be rolled up on the arm. *(When dealing with the public, tie must be on unless wearing a BHPD issued turtleneck.)*

3. **SUMMER DUTY UNIFORM Class "1"** - Short sleeve gray 'Flying Cross-Duro Poplin' 65% Dacron Polyester 35% Cotton #35W5441, navy blue freedom fit by 'Fechheimer' poly-wool blend pants with silver stripes #RN28562 may be worn on or after March 1<sup>st</sup>, at the discretion of the Agency's 2<sup>nd</sup> in command. On and after April 1<sup>st</sup>, until October 1<sup>st</sup>, the summer uniform shall be worn. This is the regular duty uniform for all Patrolpersons in summer.

4. **WINTER DUTY UNIFORM Class "2"** - Long sleeve gray uniform shirts Tactical 'Tru-Spec' 65% Dacron Polyester 35% Cotton #1416, without tie, and black 'Tru-Spec' #1062 Tactical pants may be worn beginning October 1<sup>st</sup>, at the discretion of the Agency's 2<sup>nd</sup> in command for evening/midnight shift. On and after November 1, until March 1<sup>st</sup>, the winter duty uniform shall be worn. This is the regular duty uniform for all Patrolpersons in winter. When a long sleeve shirt is being worn, the sleeves will be extended their full length. At no time will the sleeves be rolled up on the arm. *(When dealing with the public, tie must be on unless wearing a BHPD issued turtleneck.)*

5. **SUMMER DUTY UNIFORM Class "2"** - Short sleeve gray Tactical 'Tru-Spec' 65% Dacron Polyester 35% Cotton #1416, and black

'Tru-Spec' #1062 Tactical pants may be worn on or after March 1st, at the discretion of the Agency's 2<sup>nd</sup> in command. On and after April 1<sup>st</sup>, until October 1<sup>st</sup>, the summer uniform shall be worn. This is the regular duty uniform for all Patrolpersons in summer.

6. A white crew neck undershirt shall be worn under the gray uniform shirt for Class "1" and black crew neck undershirt for Class "2".

7. No unauthorized jackets, sweaters, vests, hats, shirts, and pants shall be worn unless issued by the agency.

#### ***C. BATTLE DRESS UNIFORMS (BDU'S)***

The Battle Dress Uniform is not authorized as a regular duty uniform. Only officers working special assignments as directed by the Chief of Police or his designee will wear the BDU uniform. A black crew neck undershirt shall be worn under the Battle Dress Uniform shirt.

#### ***D. A complete uniform shall be worn.***

When required and no item of the uniform shall be worn except as part of the complete uniform.

1. Wearing of the uniform jacket with civilian clothes is prohibited.

2. Wearing of the uniform pants with a non-uniform shirt is prohibited.

3. No substitutions for uniform equipment shall be allowed unless specifically approved by the Chief of Police in writing.

#### ***E. PATROL DIVISION EXCEPTION***

1. Patrol Division may, at the discretion of the Chief of Police, or Agency's 2<sup>nd</sup> in Command may wear the long sleeve dark

navy uniform sweater for the winter duty uniform and long sleeve gray shirts for the winter.

2. This uniform exception may be modified or changed at the discretion of the Chief of Police without altering the concept or intent of this policy.

#### **V. INSIGNIA**

A. Designated shoulder patches and appropriate rank insignia shall be worn on all shirts and coats.

1. Berwyn Heights Police Department patch on both sleeves.

2. Accessory items, to include rank insignia, medals and accouterment shall be worn as part of officer's uniform. Officers shall have one week after promotion to display their ranks.

#### ***I. NON-UNIFORMED PERSONNEL***

1. Investigative Services Section Class "3".

a. During winter months, as specified above, all detectives will wear a long sleeve button down shirt, and slacks. When a long sleeve shirt is being worn, the sleeves will be extended their full length. At no time will the sleeves be rolled up on the arm. The embroidering of a badge and the investigators name and rank on the shirt is authorized.

b. During the summer month's detectives, in lieu of the long sleeve button down shirt with tie, detectives' may wear short sleeve button down shirts and slacks. The embroidering of a badge and the investigators name and rank on the shirt is authorized.

c. For sworn female detectives professional business attire will be acceptable.

d. Whether shoes or boots, footwear worn by male and female detectives shall be of a

type suitable for business attire. Shoes or boots shall be clean and free of dirt and grime and shall be polished to a smooth appearance. No athletic shoes are authorized.

e. When attending Circuit or District Court male detectives shall wear a button down shirt, tie sports coat, and slacks or a suit. Female detectives shall wear suitable business attire.

f. While assigned with the United States Secret Service, or the United States Marshal, detective may dressed as his or her assignment as to the nature of the task-force functions.

## **2. Police Service Aide (PSA)**

Civilian attire is authorization for PSA, as authorized by the Chief of Police, the Investigative Services Section, or his designee. However, all PSA must maintain the duty PSA uniforms as prescribed in the General Order Section.

## **VI. PART TIME WORK UNIFORM**

A. All officers working part time jobs shall wear the duty uniform of the day. There will be no distinction between the part time job uniform and on duty uniform requirements. Example: If the winter uniform is to be worn while on duty, it will be worn on part time jobs also. (There is currently no part-time employment outside of the incorporated Town limit at this time without prior approval from the Chief of Police.)

B. The policy for the wearing of civilian clothing during part time employment at part time jobs must be approved by the Chief of Police or his designee.

## **VII. TURTLENECK SWEATERS**

A. The optional wearing of turtleneck sweaters with an open collar on long sleeve shirts during the winter uniform period is authorized. Black turtleneck with 'BHPD' to the left of the collar will be the only sweater authorized for all officers.

## **VIII. UNIFORM/EQUIPMENT**

A. All personnel will be held personally accountable for the return of all department issued uniform items and/or equipment. No issued item is to become the property of any individual; all remain the property of the BHPD.

B. Items lost or damaged during law enforcement activities will be documented on a report and forwarded through the chain of command to their supervisor.

C. Replacement of items of personal purchase which are lost or damaged in law enforcement activities will be determined on a case-by-case basis.

D. Property lost or damaged as a result of law enforcement activities in connection with an arrest of an individual will be promptly reported, replacement costs determined, and the officer involved will include, during prosecution of the individual, a request to the courts that any sentence include reimbursement of costs to the department.

E. All officers will be issued a body armor vest and carrier for use. Wear will be required for all personnel participating in raids, and barricade or hostage situation, search warrant entry, or in any situation deemed appropriate by the Chief of Police. Wear at other times is strongly recommended.

## IX. DUTY BELTS

A. All uniform officers will wear a full gun belt while on duty.

B. A full gun belt is considered to be an outer belt, at least 1 ¾ inches in width, worn over the trouser belt designed to hold additional equipment and will consist of a holster, either jacket slot or high-rise, that has a strap over the top of the weapon with a thumb break retention system, or greater (ex: level 2 or 3), at least one magazine pouch designed to hold a minimum of two additional magazines that have straps or covers to retain the magazines, and a handcuff pouch that will hold a minimum of one pair of handcuffs.

C. Additional equipment may be worn on the full gun belt as long as the equipment is fully enclosed and secured and will not come off the belt during police activity. The full gun belt will be secured to the trouser belt by no less than four "keepers", two in front and two in back.

D. At no time will an on-duty officer wear a tactical thigh holster as a regular duty holster. Tactical thigh holsters are only permitted for use by the Special Operation while serving warrants and detective while serving warrants. Uniform officers with a primary office or desk assignment are not required to wear a full duty belt.

E. Officers assigned to an office or desk assignment can wear a holster, with a minimum of a thumb break retention system, attached to the trouser belt and must have at least one spare magazine and be equipped with handcuffs. This does not apply to Patrol supervisors who may be required to answer calls for service. All patrol division officers will wear a full gun belt.

F. Officers, while on duty and dressed in civilian clothes, shall wear a primary handgun in a holster secured with a minimum of a thumb break retention

system. A holster of greater retention is permitted. A departmental badge shall be displayed on the officer's weapon side anytime a weapon is visible. Also, any plain clothes officer will have an extra magazine and be equipped with handcuffs.

G. Officers while off duty are encouraged to carry their handgun with them. While off duty the weapon "must" be concealed from public view. Uniform patrol officers attending court are considered to be on duty and may wear a visible primary sidearm while in uniform. The weapon must be secured in a holster with a minimum of a thumb break retention system and the officer must be equipped with an extra magazine and handcuffs. A departmental badge will be displayed on the weapon side. Any officer working a part-time job and has been approved by the Chief of Police to work in plain clothes may also wear a visible primary sidearm under the same requirements.

H. No officer will be armed while under suspension, unless possession of a firearm is in compliance with existing state statutes regarding the use and possession of firearms by the general public.

I. A primary handgun shall not be worn on the gun belt in a holster or other device which places the handle of the weapon more than three (3) inches from the body. When the handle of the weapon is tilted forward and away from the officer's body, the weapon can hang on doors, windows, belts, etc., and makes it possible for another person to take the firearm away from the officer.

J. Cross-draw or swivel holsters will not be worn on the duty belt. Cross-draw concealed holsters worn from a suspension device may be used as long as the holster has a minimum of a thumb break retention system. Cross-draw holsters are permitted on tactical vests worn by the Investigative Services while serving warrants or detective while serving warrants.



- Exception: Officers authorized to deploy and issued the department approved Electronic Restraint Device-Taser will adhere to the Berwyn Heights Police General Order # TBA in reference to the wearing and deployment of the device and its holster.

## **X. FOOTWEAR**

A. Shoes or boots worn with the authorized uniform of the day must be black smooth grain leather or similar synthetic material having an acceptable likeness to leather with a plain toe. (No tennis shoes, loafers, wing tips or shoes or boots with ornamental designs). The heel shall not exceed 1-1.2 inches in height.

B. Shoes or boots shall be clean and free of dirt and grime and shall be polished to a smooth blackened appearance.

## **XI. SOCKS**

Socks worn with low cut shoes shall be black or navy blue. White socks may be worn for health reasons when supported by a physician's statement, or wearing boots.

## **XII. BADGES**

A badge and hat shield shall be issued to every officer. The hat shield shall be worn attached to the front of the hat, when in uniform. The badge shall be worn over the left breast, while attired in uniform unless the garment has an authorized badge patch. Officers working in plain clothes shall display their badge openly when their firearm is in view. No Unauthorized badges shall be worn or displayed.

## **XIII. WINDBREAKER TYPE OUTERWEAR**

For a uniform and standardized image this department is authorizing the Blauer / Flying Cross Police Windbreaker for wear in inclement weather. Other windbreaker type jackets, even if not the Blauer / Flying Cross brand, must present this type of style and appearance. Other assorted black "Police" windbreakers, and other light jackets currently worn that do not meet these specifications, will not be authorized. Patches and insignia shall be required and worn as per departmental regulations.

<b>Title:</b>	<b>Body Armor</b>	<b>Order #</b>	<b>1-600.1</b>
<b>New/Amends/Resc:</b>	<b>New</b>	<b>Page:</b>	<b>01</b>
<b>Approved by:</b>	<b>Chief Ken K. Antolik</b>	<b>Officer Signature:</b>	
<b>Effective Date:</b>	<b>July 01, 2011</b>		
<b>Review Date:</b>			

## **I. PURPOSE**

The purpose of this policy is to provide the BHPD officers with guidelines for the proper use and care of body armor.

## **II. POLICY**

It is the policy of the BHPD to maximize officer safety through the use of body armor in combination with prescribed safety procedures. While body armor provides a significant level of protection, it is not a substitute for the observance of officer safety procedures.

## **III. DEFINITIONS**

**Field Activities:** Duty assignments and/or tasks that place or could reasonably be expected to place officers in situations where they would be required to act in enforcement rather than administrative or support capacities.

## **IV. PROCEDURES**

### **A. Issuance of Body Armor**

1. All body armor issued must comply with protective and related requirements prescribed under current standards of the National Institute of Justice.
2. All officers shall be issued agency-approved body armor.
3. Body armor that is worn or damaged shall be replaced by the agency. Body armor that must be replaced due to misuse or abuse by the officer shall be paid for by the officer.

### **B. Use of Body Armor**

1. Officers shall wear only agency-approved body armor.

2. Body armor shall be worn by all probationary officers during field training.

3. Officers that are assigned to a uniformed function and non-uniformed sworn officers are required to wear body armor while engaged in field activities both on duty and during off duty employment unless exempt as follows:

- a. When an agency-approved physician determines that an officer has a medical condition that would preclude wearing body armor.
- b. When the officer is involved in undercover or plain clothes work that his/her supervisor determines could be compromised by wearing body armor; or
- c. When the department determines that circumstances make it inappropriate to mandate wearing body armor.

### **C. Inspections of Body Armor**

1. Supervisors shall be responsible for ensuring that body armor is worn and maintained as required by this policy through routine observation and periodic documented inspections.

2. Annual inspections of body armor shall be conducted for fit, cleanliness, signs of damage, abuse and wear.

### **D. Care, Maintenance and Replacement of Body Armor**

1. Officers shall routinely inspect personal body armor for signs of damage and for general cleanliness.
2. As dirt and perspiration may erode ballistic panels, each officer shall be responsible for cleaning personal body armor in accordance with the manufacturer's instructions.
3. Officers are responsible for the proper storage, maintenance and care of body armor in accord Model Policy.

4. Officers are responsible for reporting damage or excessive wear to the ballistic panels or cover to their supervisor and the individual responsible for the uniform supply function.

5. Body armor will be replaced in accordance with guidelines and protocols established by the National Institute of Justice.

#### E. Supervisors

The Supervisors shall be responsible for:

1. Monitoring technological advances in the body armor industry that may necessitate a change in body armor.

2. Assessing weapons and ammunition currently in use and the suitability of approved body armor to protect against those threats.

### V. CARE, CLEANING AND REPLACEMENT

Although body armor is capable of stopping bullets, it is far from indestructible. Damage is not always readily visible, and an officer could wear a damaged, ineffective vest in the mistaken impression that it is serviceable. This is why it is extremely important that proper cleaning and care practices be observed.

Body armor should be protected from sunlight or any other source of ultraviolet light, as it breaks down the ballistic resistance of vest materials. Officers should be instructed never to leave body armor in vehicles exposed to sunlight and that outdoor drying of armor following cleaning is strictly prohibited.

Damaged armor may have a slight color change and appear browner, although damage can occur without visible detection.

Dry cleaning solvents, harsh detergents, and bleach can also damage body armor. Bleach is probably the most severe, even in very diluted amounts. Milder detergents of the home variety are safe, but stronger detergents common to commercial laundering, as well as some dry cleaning solvents, can cause damage. It is strongly recommended that commercial laundering of body armor be avoided. Home washing should be performed by hand, since tests have suggested that armor is damaged by machine washing, and possibly by machine drying as well.

Body armor should be gently washed by hand with mild soap and water. Washing will not affect the water-repellency of the armor, and full ballistic capability will return once the armor has dried. However, care should be taken to thoroughly rinse all soap residues from the armor, as they may accumulate over time and absorb enough water to impair ballistic efficiency. After the armor is washed, it should be hung indoors. Armor should never be hung on outside clotheslines, whether in the shade or on a cloudy day.

In addition, the officer should inspect the armor after it has been washed for signs of damage or wear. One should look for fraying, cuts, stains, fading (indicating possible bleach damage), and "browning" (indicating possible ultraviolet light degradation).

Moreover, the BHPD shall conduct annual or semiannual inspections of the armor to ensure that proper care is being taken and that the armor is serviceable. Many agencies find it convenient to inspect body armor in conjunction with routines established for firearms qualifications.

In addition to periodic visual inspections of armor, the BHPD may consider conducting tests of armor for ballistic efficiency. Unless the department has adequate resources and equipment,

A list of 7 approved laboratories can be obtained by contacting the National Law Enforcement and Corrections Technology Center, Rockville, Maryland, at 1-800-248-2742 or by mail at the address provided at the end of this document.

However, if the sample armor fails the test, further tests should be conducted with an eye towards possible replacement of all vests of comparable stock. Failure of one vest sample may be a matter of statistical chance and not an indication that an entire lot should be replaced or discredited. Additional test failures would strongly suggest that replacement is in order or that another vest model should be considered.

Procurement of body armor should not be regarded as a one-time purchase. Regular periodic replacement should be based on more than concerns for ballistic efficiency.

Factors such as changes in types of weapons and ammunition commonly found in a community, improvements in body armor technology, and the changing physical characteristics of officers should also be considered.

When these factors are considered, replacement of existing armor may be appropriate regardless of the continued efficiency of older armor.

Finally, armor that is shot in the line of duty, as well as the armor used in tests, must be permanently retired. Because body armor is very difficult to cut, will not burn and cannot be incinerated there are serious limitations on disposal methods. It is recommended that disposal of retired armor be carefully monitored to prevent the possibility of later use by criminals. Disposal in landfills is not recommended for this reason and the fact that ballistic material is not biodegradable.

It is recommended that a BHPD Supervisor or the Chief of Police contact the armor manufacturer to determine if they maintain a disposal facility for use of their clients.

Also, the BHPD may consider using old body armor to provide ballistic resistance in areas that may need but may not have such capability. For example, used body armor may be installed in the door panels of police vehicles, behind desks that are exposed to the general public, as part of partitions in police work stations.

**NO USED / EXPIRED BALLISTIC VESTS SHALL BE GIVEN OUT TO CIVILIANS OR NON LAW ENFORCEMENT AGENCIES.**

#### **References and Addresses:**

■ For information regarding the IACP/DuPont Kevlar Survivor's Club®, contact:  
IACP/DuPont Kevlar Survivor's Club,®  
Club Administrator

5401 Jefferson Davis Highway  
Richmond, VA 23234  
1-800-441-2746

E-mail: [survivor@usa.dupont.com](mailto:survivor@usa.dupont.com)

■ For NIJ publications cited in this paper (the 0101.06 NIJ standard, the consumer product list, and the armor selection guide), contact:

National Institute of Justice (NIJ)  
National Criminal Justice Reference Service  
P.O. Box 6000  
Rockville, MD 20849-6000  
1-800-851-3420 e-mail: [askncjrs@ncjrs.org](mailto:askncjrs@ncjrs.org)  
To access them on the World Wide Web site, use:  
<http://www.ncjrs.org>

■ For information on testing protocols and body armor standards, contact:

National Law Enforcement and Corrections Technology Center  
P.O. Box 1160  
Rockville, MD 20849-1160  
Tel: 1-800-248-2742; or 1-301-519-5060  
World Wide Web address: <http://www.nlectc.org>



<b>Title:</b>	<b>Transponder 'EZ-Pass'</b>	<b>Order #</b>	<b>1-600.2</b>
<b>New/Amends/Resc:</b>	<b>New Amended</b>	<b>Page:</b>	<b>01</b>
<b>Approved by:</b>	Chief Ken K. Antolik	<b>Officer Signature:</b>	
<b>Effective Date:</b>	July 01, 2013		
<b>Review Date:</b>			

#### **I. PURPOSE**

The purpose of this policy is to set forth guideline to standardize the policy and procedures for proper usage of the State issued Transponder 'EZ-pass'.

#### **II. POLICY**

It is the policy of this agency that all personnel will properly utilized the State issued Transponder 'EZ-Pass'.

- a. The use of the State issued Transponder 'EZ-Pass' for personal commuting expenses violates the policy set forth in under Order # 1-600.2.
- b. The use of attending non-business events or personal use. The policy defines "personal use" to exclude commuting between home and the employee's office.
- c. An employee assigned with the Transponder 'EZ-pass' must use the vehicle for official business and commuting purposes excluding for personal travel on weekends and holidays unless the employee is schedule to work or responding to an emergency during the aforementioned holidays, or exigent circumstances.

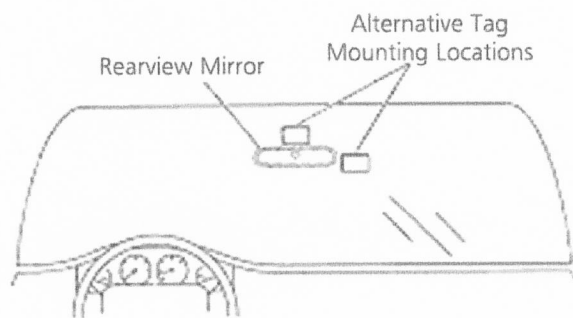
#### **III. WINDSHIELD MOUNTED TRANSPONDER**

As your vehicle enters the toll lane, the transponder EZ-Pass that is mounted on your vehicle's windshield is read by the antennae. As your vehicle passes through, your Transponder 'EZ-pass' account is charged the proper amount. If your vehicle does not have a transponder, the system classifies you as a violator and cameras take photos of your vehicle and your license plate for processing. The Transponder 'EZ-pass' must be mounted properly before use. If the transponders is not properly mounted, it may not work and may be unlawfully positioned.

#### **IV. MOUNTING**

- 1.Clean placement area on inside of windshield with isopropyl (rubbing alcohol) and allow to dry.
- 2.Remove plastic tape from back of mounting strips on transponders.
- 3.Position transponders as illustrated below based on your mirror type.
- 4.Press transponders firmly against the windshield glass.

For BHPD vehicles, please mount transponders as shown below:



# CHART ON THE DIFFERENT MUNICIPAL AGENCIES TAKE HOME CAR PROGRAM

RIVERDALE	30 AIR MILES	TO AND FROM WORK/WORK RELATED	\$22.50 BIWEEKLY	NO
TAKOMA PARK	50 AIR MILES	TO WORK AND HOME/RELATED PERSONAL BUSINESS	NO	NO
UPPER MALBORO	25 AIR MILES	TO AND FROM WORK/ PART TIME	\$10 PER WEEK IF IT MORE THAN 25- 30 MILES	NO
EDMONSTON	25 AIR MILES	MORE THAN 25 AIR MILES IT CAN BE PARKED AT A CLOSE FD OR PD	BETWEEN \$10-25 BIWEEKLY DEPENDING ON LOCATION	NO
BOWIE	20 AIR MILES	INSIDE THE CITY PERSONAL /OUTSIDE THE CITY WORK AND HOME	NO	NO
COLMAR MANOR	IN PG COUNTY ONLY	BUSINESS USE ONLY	PAY FOR OIL CHANGES, ROUTINE MAINTENANCE	NO
UNIVERSITY PARK	25 AIR MILES	TO AND FROM WORK/POLICE RELATED	NO	NO
CHEVERLY	25 AIR MILES	TO AND FROM WORK/ PART TIME	NO	NO
SEAT PLEASANT	25 ROAD MILES	TO AND FROM WORK/PERSONAL USE	PAY FOR OIL CHANGES, PAY FOR GAS IN EXCESS OF 90 GALLONS PER MONTH	NO

<b>Title:</b>	<b>Take Home Police Vehicle</b>	<b>Order #</b>	<b>1-600.3</b> <b>[See Council Rule #19]</b>
<b>New / Amends / Resc:</b>	<b>New-Revised</b>	<b>Page:</b>	<b>01 of 03</b>
<b>Approved by:</b>	<b>Chief Ken K. Antolik</b>	<b>Officer Signature:</b>	
<b>Effective Date:</b>	<b>July 01, 2011</b>		
<b>Review Date:</b>	<b>September 23, 2013</b>		

### **01 Purpose:**

To establish criteria for general regulations pertaining to take-home vehicles.

### **02 Policy:**

It is the policy of the 'BHPD' Berwyn Heights Police Department to provide take-home vehicles to sworn personnel. Only officers who are eligible for the take home car program may not use the vehicle for off-duty personal use.

### **03 Eligibility:**

A. Basic Eligibility: An Officer shall be eligible for a take home vehicle after successful completion of Field Training, unless authorized by the Chief of Police, or his designee.

B. Officers who reside within the Town limits and Officers who reside within 30 road miles of the edge of Town's jurisdiction shall be provided a take home vehicle.

C. Officers who do not qualify under any of the above categories on the date of this Agreement but who, as of the date of this Agreement have been provided a take home vehicle shall continue to be provided a take home vehicle. Provided, however, such Officer shall lose the availability of a take home vehicle when;

The Officer moves his/her residence further away from the center point/edge of Town than his/her current residence; or,

The Officer changes duties to a position, which does not qualify for a take home vehicle.

D. The use restrictions described in this Article do not apply when or at such time as:

The Officer has been designated as Active On-Call, and the Officer is in fact On-Call; and,

The Officer is traveling to and from police related Secondary Employment (in Town), Department Training and work related Court Appearances.

E. Officers are allowed, within reason, to stop briefly, en route, to and from their official designation prior to and or after their assignment of duty.

F. Departmental Take-Home Vehicle will not be left unattended with the engine running for any period of time with or without key/transponder.

G. Departmental Take-Home Vehicle will not be left at any location for the purpose of the officer / employee receiving money, goods, service, or profit of any kind, because of that vehicle's placement.

H. The officers participating in the aforementioned program are restricted to the use of the Take-Home vehicle for Official Business only, i.e. back and forth to work, to Court, to conduct investigations and any prior approval from their supervisor(s) or the Chief of Police. [ prior approval must be in written memo ]

### **NOTE:**

*The Take-Home program is subject to approval of the Town Council and the Chief of Police, and may individually or summarily be limited, suspended or revoked as may, in their opinion, be in the best interests of the Town of Berwyn Heights, Maryland.*



#### **04 GENERAL REQUIREMENTS:**

A. Take-home cruisers may be used for transport to places of employment by off-duty police officer privately employed (in Town). However, if the private employer requires the use of a cruiser for security patrolling or other purposes, the approval of the Chief for such use shall be first obtained and the Town may require reimbursement for vehicle expenses incurred.

B. When the officer is off-duty and in the vehicle, the officer must be armed with an approved weapon and utilized seatbelt / shoulder harness combination properly. (as instructed in the vehicle manual ).

C. When operating the vehicle off-duty, the police radio must be kept on. Officers are expected to aid disabled motorists and to provide back up to on-duty personnel in need of assistance.

D. Officers approved to have take home vehicles will remain within 30 miles of the Town unless authorized by the Chief of Police or his/her designee.

**NOTE:** *Officers on official police business may leave the State of Maryland (i.e., approved training, conferences, etc.).*

E. In minor cases encountered off-duty, the officer may call for a beat officer to handle the matter. If immediate action is necessary, the off-duty officer will handle the situation.

F. Officers may not transport persons other than Town employees in vehicles assigned as take home vehicles unless is part of work assignment. These people include friends, family members, and other persons that the officer might normally transport in his/her personally owned vehicle. Children shall not be transported, except in an emergency, unless they are restrained as required by the Maryland Vehicle Law.

G. While on leave in excess of five days, whether sick leave, annual leave out of town or administrative leave other than for training purposes, officers must arrange for delivery of the vehicle to the BHPD. If an officer is so ill they cannot bring his/her car to the station, arrangements will be made to have the vehicle picked up.

H. Officers whose police powers have been suspended must deliver the vehicle to the BHPD.

I. Officers are prohibited from purchasing alcoholic beverages at drive-up windows while operating a Departmental vehicle.

J. Operation of Departmental vehicles by personnel who have consumed alcoholic beverages, or CDS is prohibited.

**05 LIGHT-DUTY ASSIGNMENTS:** Officers on light-duty are not eligible to participate in the Take Home Car Program. The Program was initiated to create a greater police presence. If an employee cannot function as an officer due to injury, the effectiveness of the program is negated. Secondly, placing an officer in a cruiser may imply in a legal sense that the officer is capable of taking action which could further injure the officer.

#### **06 MAINTENANCE AND EQUIPMENT:**

A. Officers are responsible for scheduling preventive maintenance and care of the vehicle. All maintenance and service will be performed at the Greenbelt Road Shell. Issued weapons such as shotguns and nightsticks, etc. will be removed from the vehicle when it is left for service.

B. Officers shall keep their cars clean, when feasible and shall report any damage to their assigned vehicle promptly.

C. Officers shall replenish supplies used during the normal course of their duties promptly.

D. Officers shall report any equipment that is lost or missing in a timely fashion and request a replacement item.

E. Non-original equipment shall not be installed in, or attached to, any vehicle unless authorized by the Chief of Police or his Second in Command.

F. The BHPD Second in Command oversees the installation of any electrical equipment authorized by the Chief of Police or his designee.

**EXCEPTION:** *The Chief of Police or the Second in Command may approve an outside contractor to install electrical equipment in police vehicles.*

**07 SMOKING:** Smoking is prohibited in Town vehicles.

**08 ADMINISTRATIVE SANCTIONS:**

A. Administrative removal from the take-home car program is authorized in circumstances wherein an officer is deemed to have been neglectful or abusive in the use of his/her assigned vehicle.

B. The take-home car program is a benefit and a responsibility. Its use is considered a privilege and not a right. As such, officers who violate this policy may be subject to removal from the program.

**09 Fueling:**

- A. Employees shall utilize an authorized vendor to obtain fuel at the lowest grade octane to keep the cost down. The current vendor is Shell Gas.
- B. The receipts shall be turned in along with the ~~daily log sheet at the end of tour of duty time~~ sheet along with your Court disposition Log.

**10. Departmental Accident:**

1. When a departmental accident is involved, the operator will immediately notify the Communications Section of the police jurisdiction in which the accident occurred.

2. The following reports must be completed by the involved officer/employee;

- Commander's Log
- Maryland Automated Accident Report (MAARS Form MSP #1)
- Photographs showing the vehicular and property damage and the geographical layout of the scene.
- Supervisor shall be notified immediately unless the officer / employee is incapacitated.
- All weapons, microphone to the mobile police radio, confidential materials and EZ-Pass Transponder shall be removed from the vehicle prior to the vehicle being towed or left for repairs.

## COUNCIL RULES

### Council Rule #19 - Police Cruisers - Maintenance, Accident Reports and Take - Home Policy

#### A. Maintenance and Equipment

1. Officers are responsible for maintenance and care of Police Department vehicles. Issued equipment such as shotguns, flashlights, night sticks, etc., will be removed from the vehicle when it is left for service.
2. Non-original equipment shall not be installed in, or attached to, any vehicle unless authorized by the Chief of Police. Furthermore, officers shall not:
  - a) place or hang any item on the inside rear view mirror, or bracket.
  - b) place any object on top of the dashboard while the vehicle is in motion.
  - c) affix any object, clip or holder to the front of the dashboard.
  - d) hang or mount any radar device, camera, or other device within the deployment of the air bags.
  - e) mount or display toys, symbols, or pennants anywhere in or on the vehicle.
3. The vehicle maintenance officer must oversee the installation of any electrical equipment, and record keeping of vehicle maintenance, as authorized by the Chief of Police.
4. Prince Georges County Automotive Services *is the preferred vendor to* oversee and provide general maintenance of departmental vehicles.

#### B. Fueling

1. Employees shall utilize an authorized vendor to obtain fuel.
2. The receipts shall be turned in along with the Daily Log Sheet at the end of the officer's *tour of duty*.

#### C. Departmental Accidents

1. When a departmental vehicle is involved in an accident, the operator will immediately notify the Communications *Section of the police jurisdiction in which the accident took place*.
2. The following reports must be completed by the involved employee:
  - a) Commander's Log
  - b) *Maryland Automated Accident report (MAARS Form MSP #1)*
  - c) Photographs showing the vehicular and property damage and the geographical layout of the accident scene.

*Heights Police Department.*

7. *Vehicles will not be driven to any secondary employment unless authorized by the Chief of Police.*
8. *Vehicles will not be left unattended for any prolonged period. Vehicles will not be left at any location for the purpose of the employee receiving money, goods, services, or a profit of any kind, because of that vehicle's placement.*
9. *No person, other than a BHPD employee, or a mechanic who must test drive the vehicle as part of authorized repair work, will be allowed to operate Agency vehicles.*
10. *Animals will not be transported in an Agency vehicle unless the animal is a Police K-9 dog, or the animal is being transported for medical treatment, or in an emergency.*
11. *The existence and conditions of a Take Home Car for the Chief of Police are subject to the terms of the Chief's hiring agreement.*
12. *When operating any Agency vehicle, the officer must be armed with an approved weapon.*
13. *Employees operating Agency vehicles shall wear the available seat belt or seatbelt / shoulder harness combination. Children shall not be transported, except in an emergency, unless they are restrained as required by Maryland Vehicle Law.*
14. *When operating the vehicle off-duty, the police radio must be kept on, and the frequency of the police jurisdiction the vehicle is in must be monitored. Officers are expected to provide back-up to on-duty personnel in need of assistance.*
15. *In minor cases encountered off-duty, the officer may call for a beat officer to handle the matter. If immediate action is necessary, the off-duty officer will handle the situation. The off-duty officer shall then assure that the matter has satisfied all provisions set forth under Art 27 Sec 594B, and Article 88. Note - The extra jurisdictional powers of Art 27 Sec 594B give an officer the power of arrest outside his/her jurisdiction in an emergency. Emergency is defined as a crime in progress which threatens the property or welfare of any person, but specifically excludes Motor Vehicle Offenses.*
16. *While on leave in excess of three (3) days, whether sick leave, annual leave out of town, or administrative leave other than for training purposes,*



officers must arrange for delivery of the vehicle to the Police Department.

17. Officers whose police powers have been suspended must deliver the vehicle to the Chief of Police.
18. Officers are prohibited from purchasing alcoholic beverages at drive-up windows while operating an *Agency* vehicle, and the operation of *Agency* vehicles by personnel who have consumed alcoholic beverages is prohibited.
19. *Officers operating Agency vehicles off-duty will be attired in a fashion which will not bring discredit to the Police Department. Clothing and footwear will be functional; i.e., it should allow the employee to perform a duty required of his position, the same as if the employee were in an on-duty status. Employees should be prepared to fulfill their on-duty responsibilities whenever they arise while the employee is operating an Agency vehicle off-duty.*
20. *Officers will keep track of their vehicle's mileage on a monthly basis, and will report the mileage on their Monthly Performance Report.*