TITLE 6

Records; Release of Information Communications; Computer Use

Title 6 ▸ Chapter 1

Access to Personnel Records by a Department Member

Sec. 6-1-1 Access to Personnel Records by the Employee.

POLICY:

(a) The City of Stanley Police Department shall, upon the request of a Department employee, permit the employee to inspect any personnel documents which are used or which have been used in determining that employee's qualifications for employment, promotion, transfer, additional compensation, termination or other disciplinary action, and medical records, except as provided in Sections 6-1-3 and 6-1-4. The Department may require the employee to make the request in writing. An employee, under Sec. 103.13, Wis. Stats., may request the inspection of all or any part of his or her records, except as provided in Section 6-1-4.

(b) Under the provisions of Sec. 103.13, Wis. Stats., the Department, at a minimum, shall grant at least two (2) requests by an employee in a calendar year, unless otherwise provided in an employment agreement, to inspect the employee's personnel records as provided in this Section. The Department shall provide the employee with the opportunity to inspect the employee's personnel records within seven (7) working days after the employee makes the request for inspection. The inspection shall take place at a location reasonably near the employee's place of employment and during normal working hours. In any case, the Department may allow the inspection to take place at a time other than working hours or at a place within Department facilities other than where the records are maintained if that time or place would be more convenient for the employee.

Sec. 6-1-2 Personnel Records Inspection by an Employee's Representative.

POLICY:

Under Sec. 103.13, Wis. Stats., an employee who is involved in a current grievance against the Department may designate, in writing, a representative of the employee's union, collective bargaining unit or other designated representative to inspect the employee's personnel records which may have a bearing on the resolution of the grievance, except as provided in Section 6-1-4. The Department shall allow such a designated representative to inspect that employee's personnel records in the same manner as provided under Section 6-1-1.

Sec. 6-1-3 Medical Records Inspections.

POLICY:

Under Sec. 103.13, Wis. Stats., the right of the employee or the employee's designated representative under Section 6-1-2 to inspect personnel records under this policy includes the right to inspect any personnel medical records concerning the employee in the Department's files. If the Department believes that disclosure of an employee's medical records would have a detrimental effect on the employee, the Department may release the medical records to the employee's physician or through a physician designated by the employee, in which case the physician may release the medical records to the employee or to the employee's immediate family.

Sec. 6-1-4 Statutory Exceptions to an Employee's Right to Inspect His or Her Personnel Records.

POLICY:

Under the provisions of Sec. 103.13(6), Wis. Stats., the right of the employee or the employee's designated representative to inspect his or her personnel records does not apply to:

(a) Records relating to the investigation of possible criminal offenses committed by that employee.

(b) Letters of reference for that employee.

(c) Any portion of a test document, except that the employee may see a cumulative total test score for either a section of the test document or for the entire test document.

(d) Materials used by the Department for staff management planning, including judgments or recommendations concerning future salary increases and other wage treatments, management bonus plans, promotions and job assignments or other comments or ratings used for the Department's planning purposes.

(e) Information of a personal nature about a person other than the employee if disclosure of the information would constitute a clearly unwarranted invasion of the other person's privacy.

(f) Records relevant to any other pending claim between the Department and the employee which may be discovered in a judicial proceeding.

Sec. 6-1-5 Corrections to Personnel Files.

POLICY:

Under Sec. 103.13(4), Wis. Stats., if the employee disagrees with any information contained in the personnel records, a removal or correction of that information may be mutually agreed upon by the Department and the employee. If an agreement cannot be reached, the employee may submit a written statement explaining the employee's position. The Department shall attach the employee's statement to the disputed portion of the personnel record. The employee's statement shall be included whenever that disputed portion of the personnel record is released to a third party as long as the disputed record is part of that file.

Sec. 6-1-6 Access by Others to an Employee's Personnel File.

POLICY:

(a) The Chief of Police, members of the Common Council, or designated authorities actually engaged in disciplinary action procedures or performance evaluations are permitted to have access to personnel records of employees in the Department.

(b) With the exception of Subsections (a) and (c), the Department shall reveal no information to others without the employee's signature on a release. This applies to requests for information from anyone or any organization, including other government agencies.

(c) Employment information will not be released without the authorization of the individual concerned, except for the following:

(1) "Directory" information which consists of verification of employment or past employment, dates of employment, position held or location of employment.

(2) When required as part of an established statutory reporting procedure.
(3) To protect the legal interests of the Department when the actions of an individual appear to violate the conditions of employment or threaten physical injury to members of the general public, to other employees or to Department property.
(4) When requested as part of an appropriate governmental inquiry into the Department's employment practices.

Title 6 ▸ Chapter 2

Release of Information

Sec. 6-2-1 Request for Information/Release of Information.

POLICY:

The City of Stanley Police Department recognizes that the public has a compelling interest in the inspection of public documents and records and in the release of information dealing with law enforcement activities. Only if there is a countervailing interest of the same or greater magnitude will anyone be denied information or the opportunity to inspect public documents.

PROCEDURES:

(a) Information released shall only be true information received by the Department. Employees releasing information shall refrain from adding information that could be construed as being opinion or gossip. A request form shall be completed for accuracy purposes.

(b) Under no circumstances will information provided to the Department by another agency or jurisdiction be commented upon or released by Department members.

COMMENTARY:

The news media and members of the general public often direct inquiries to the Department seeking information on a variety of subjects. While it is the desire of the Department to fulfill such requests, it is not always possible to do so. The decision to release information or to grant interviews shall be determined on a case-by-case basis.

Section 19.21, Wis. Stats., states that any person may, with proper care, during office hours and subject to such orders or reasonable regulations as the custodian thereof prescribes, examine or copy any property or things in the legal possession or control of each and every officer of any governmental unit and his deputies. The statute also provides that any person may, at his own expense and under such reasonable regulations as the custodian prescribes, copy or duplicate any materials, including, but not limited to, blueprints, slides, photographs and drawings.

This statute was construed and applied to law enforcement agencies in *Beckon v. Emery,* 36 Wis. 2d 510 (1967), where a balancing test was established. The test is that the public interest favors public inspection, but if the requested disclosure would do more harm to the public interest, the request may be reasonably denied. (See special memoranda no. 49 and no. 50, Office of Attorney General, *Wisconsin Law Enforcement Bulletin,* November 15 and December 15, 1967. Both the statute and the Attorney General's decisions establish the policy that the public has a right to know, absent exceptional circumstances. The policy legitimately extends to all publicly held information, regardless of whether it has been reduced to written form.

Sec. 6-2-2 Release of Information Pertaining to an Arrest or Prosecution.

PROCEDURES:

(a) The following information about an arrest will be released upon request:

(1) The arrested person's name, age, residence, employment, marital status and similar background information.
(2) Information summarizing the offense or charge.
(3) The circumstances immediately surrounding the arrest, including the time and place of the arrest, resistance, if any, possession of weapons, the use of force and a description of items seized at the time of the arrest.

(b) The following information will *not* be released:

(1) Observations about an arrested person's character, criminal or arrest record, criminal involvement or guilt.
(2) Statements concerning the identity, credibility or testimony of prospective witnesses.
(3) Statements concerning evidence or argument in the case regardless of whether it is anticipated that such evidence or argument will be used at trial.
(4) Comments about whether an arrested person has made an admission or confession or given an alibi or about any other thing that might be used against him or her at a subsequent trial.
(5) Statements of any kind made by an arrested person.
(6) Anything in which investigation is pending.

(c) Information that may be released under certain circumstances:

(1) Information about evidence or witnesses will be released if authorized by the district attorney or at the trial court.
(2) The names of victims of criminal acts will be released unless such information will endanger the individual's safety, hamper further investigation, is contrary to law or a reasonable effort to notify the deceased victim's next of kin has not been made.

(d) Reports may be copied at the expense of the person making the request so long as restricted information is redacted.

COMMENTARY:

This set of procedures attempts to balance the public's right to know about criminal activity in the community or other police events with the arrested person's right to a fair trial free from undue publicity and to promote the protection of the rights of the victim. In *Newspapers, Inc., et al. v. Breier* (May 30, 1979), No. 76-274, it was decided that daily arrest records must be made available for routine inspection so the press and members of the public could ascertain the charge for which a person was arrested.

Sec. 6-2-3 Criminal Investigations and Investigative Techniques.

POLICY:

The Department will deny access to or release of information if the information would harm an ongoing investigation or the Department's investigative methods.

PROCEDURES:

Access to or release of information may be granted as soon as it would no longer be harmful to the ongoing investigation or person and if it is not prohibited by another provision of this policy.

COMMENTARY:

The effectiveness of investigative techniques and their value are decreased if current or potential lawbreakers are forewarned of their nature. Unless there is a substantial and lawful purpose, access to or release of evidentiary information relating to fingerprinting, polygraph examinations, blood alcohol tests, firearms examination, other laboratory procedures, surveillances, the use of informants, alarms and timetables for transactions or transportation of valuables and persons shall be denied.

Sec. 6-2-4 Privacy Considerations and Release of Information.

POLICY:

Information based on rumor or hearsay which would harm the reputation of any person or group in the community will not be released.

PROCEDURES:

(a) Unless there is a specific purpose, the names of persons merely suspected of a crime will not be released.

(b) The identity of complainants, informants or victims will not be released where it will hamper investigations, endanger a person's safety or is contrary to law.

(c) Statements, comments or observations about the character of fellow Officers or supervisory or command personnel will not be made.

(d) Any request for character references by anyone not representing a law enforcement or social service agency shall be denied.

COMMENTARY:

This policy and associated procedures balance the individual's right to privacy and continued enjoyment of his or her reputation with the obligation of the Department to disclose.

Sec. 6-2-5 Illegal Purpose.

POLICY:

If Department personnel have reasonable cause to believe that the access to or release of information sought will be used for illegal purposes, access to or release of information will be denied.

COMMENTARY:

This policy is particularly aimed at preventing tampering with witnesses and evidence and the protection of the safety of persons giving information to the Department.

Sec. 6-2-6 Juvenile Records.

POLICY:

The City of Stanley Police Department will deny requests for inspection of juvenile records, except to representatives of the news media who, request in writing, wishing to obtain information for the purpose of reporting news without revealing the identity of the child involved. Information on juveniles may only be exchanged between law enforcement agencies, social service agencies and the school which the juvenile attends. Requests for inspection of juvenile records will not be denied if the offense involved is a traffic violation.

COMMENTARY:

This Section is based on Sec. 48.396(1) of the Revised Wisconsin Children's Code, Wis. Stats. Under the Code, juveniles aged sixteen (16) and seventeen (17) who are handled in criminal and civil courts for certain violations are not subject to this privilege and their names may be released.

Cross-Reference: Title 6, Chapter 3, Juvenile Records

Sec. 6-2-7 Harassment.

POLICY:

If it is reasonably clear that the party requesting access is using the request as a means of harassing the Department or individual, his/her request shall be denied.

PROCEDURES:

If access is denied, the party shall be informed of the reason for the denial, but it will not be necessary to do so in writing.

COMMENTARY:

Harassment occurs if repeated requests are made having the primary purpose of annoying or impeding the functions of the Department. The request will be denied only if it is reasonably clear that harassment is the sole basis for the request.

Sec. 6-2-8 Telephone Requests for Information.

POLICY:

When the reason for the request cannot be established, information will not be released over the telephone. Criminal or investigative information shall only be released to another law enforcement agency over the telephone when that agency is recognized by the Department member receiving the call.

PROCEDURES:

In such cases, the person making the request will be asked to do so in person by coming to the Department during normal working hours.

COMMENTARY:

Requiring persons seeking access to information to appear personally helps insure that information is accurately understood.

Sec. 6-2-9 Administrative Restrictions on the Release of Information.

POLICY:

Administrative convenience may require temporary restrictions on access to information.

PROCEDURES:

(a) In such cases, the individual requesting information will be informed when the information may be obtained. The delay in such a case may not be so great as to effectively preclude the use of the information in question.

(b) Except for emergency matters and pending litigation, requests for information will be handled at the Department's earliest convenience on a first-come, first-served basis.

COMMENTARY:

This Section establishes the answer to the request for information which comes at a time when all departmental personnel are engaged in other activities and it would be extremely inconvenient to immediately fulfill the request. For example, a researcher requesting a detailed breakdown of crime statistics who first appears at the Department on a Friday evening might be asked to return on Monday morning, or to set up some other appointment.

Sec. 6-2-10 Release of Information by Permission of the Chief of Police Only.

POLICY:

Since the Chief of Police bears the full responsibility for the lawful and orderly operation of the Department, information relating to policy and procedure, interdepartmental communications, budget requests, logistics, plans, personnel matters and photographs will only be released by the Chief of Police or his/her authorized designee.

PROCEDURES:

Furthermore, information relating to cases which may involve potential civil liability for the Department should be withheld until review and approval has been obtained from the Department legal counsel. If there is reason to believe a request involves information which concerns potential liability of the Department, the person making the request should be referred to the Chief of Police.

COMMENTARY:

This Subsection seeks to insure the accuracy of information released dealing with Department-wide matters. It prohibits members of the agency from releasing such information without prior approval of the Chief of Police. Furthermore, the procedural section deals with the possibility of potential municipal liability, in which case legal advice should first be obtained from the appropriate legal counsel.

Sec. 6-2-11 Responsibility of Officers to Supply Information.

POLICY:

An Officer should appropriately answer questions put to him or her or refer the person to the proper individual or agency for such answers.

COMMENTARY:

Frequently, due to public expectations and because of his or her accessibility, an Officer is called upon to supply information both related and unrelated to the law enforcement function. It is through these contacts with the public that the Officer has a good opportunity to positively influence the public's reaction toward the Department and to enhance the image of law enforcement.

Sec. 6-2-12 Inspection Requests—Denial.

POLICY:

(a) If any of the grounds for denial of a request listed in this policy are present and applicable, the request will be denied. Reasons for the denial will be given in a courteous manner.

(b) If a Department member feels there are valid reasons for denying a request, but they are not present in this policy, the request will be forwarded to the Chief of Police along with written recommendations by the member.

Sec. 6-2-13 Availability of Records.

POLICY:

The Chief of Police is designated as the legal custodian of all Department records. Inquiries about the availability of records may be made at police headquarters during regular office hours. When records are legally available for public inspection, copies may be made per photocopy or electronic duplication at the City's current public records rate.

Sec. 6-2-14 Administrative Reports.

POLICY:

(a) **Incident Reports** are *required* to be filed, on approved forms, for all crimes, violations and complaints received or observed by members of this Department in the course of their duties, including traffic arrests.

(b) **Incident Reports** are *desired* on any matter which comes to the attention of any Officer of this Department which may later become the subject of an investigation or litigation, or which may, for a variety of reasons, be properly included in Police Department records.

(c) **Supplement Reports** are *required* to be filed, on approved forms, for any action taken, information received, or disposition made on any matter for which an Incident Report has previously been prepared.

(d) **Inventory Reports** are *required* to be filed, on approved forms, on any item recovered, seized, impounded, or taken into the custody of any Officer of this Department, in the course of duty, for any reason whatsoever.

(e) **Traffic Accident Reports** are *required* to be filed, on form MV-4000 when required by law, when a traffic accident is brought to the attention of any Officer of this Department. (See Section 6-2-15 Records Requests Involving DPPA Issues.)

(f) **Open Door Reports.** Every open door that is found will require a case and filing of an open door report on the incident report.

(g) **Alarm Report.** Every alarm that is responded to within the City will require a case and an alarm report on the incident report.

(h) **Vehicle Lock-Out Report.** Every vehicle lockout responded to shall be documented on the incident report.

Sec. 6-2-15 Records Requests Involving DPPA Issues.

COMMENTARY:

Areas of signficant legal and administrative uncertainty currently exist regarding the release of information contained in law enforcement reports pertaining to motor vehicle and driver records. The core legal issue involves how conflicting public interest policies intersect and can be properly reconciled involving the broad "right to know" scope of the Wisconsin Open Records Law with the privacy protections contained in the federal Drivers Privacy Protection Act (DPPA).

The DPPA is a federal law which protects the privacy of personal information contained in the reports of state departments of motor vehicle reports [example: Wisconsin Motor Vehicle Accident Report MV-4000]. Congress enacted the DPPA law in response to privacy concerns surrounding the use of such information collected from public records for commercial marketing and the role of such released information in criminal activities.

The federal DPPA law provides that "a state department of motor vehicles, and any officer, employee, or contractor thereof, shall not knowingly disclose or otherwise make available to any person or entity" any "personal information" or "highly restricted personal information" including:

a person's photograph, social security number, driver identification number, name, address, telephone number, and/or medical or disability information. The federal DPPA is a broad prohibition applicable to local law enforcement agencies which have access to such Department of Motor Vehicles information.

The problem is that the DPPA and the broad public access to records policies in the Wisconsin Open Records Law, while overlapping in different ways, appear to conflict in areas. The problem for how law enforcement agencies should respond to information requests involving such records has been compounded by the lack of clear published appellate court decisions. In response to this problem, many law enforcement agencies have engaged in extensive redaction of local law enforcement records being released which contain personal information so as to be cautious about not violating the DPPA. Critics of such a response policy have felt that routine redaction of all personal information from law enforcement records, regardless of where the information came from, is an overly broad response to the DPPA and may violate the Wisconsin Open Records Law.

To provide some degree of consistency in how to respond to requests for such records, the League of Wisconsin Municipalities, Wisconsin Newspaper Association, and various media, municipal, law enforcement, and municipal insurance representatives agreed in 2014 to develop an information request form (Appendix A – Limited Vehicle/Driver Record Information Request Form) to provide statewide uniformity and consistency regarding responding to such information requests.

POLICY:

The Department will utilize the Information Request Form when requests are received for the release of information which may involve DPPA concerns.

PROCEDURES:

(a) In using the Information Request Form, where a requester does not identify the information needed to release personal or highly restricted personal information, such information may not be released. Where the requestor properly completed the Information Request Form, the information may be released in unredacted form unless, based on an informal Attorney General opinion, the public records balancing test or statutory prohibitions other than the DPPA may preclude disclosure. Given the lack of clear guidance from the courts on this issue, such information requests will still be evaluated on a case-by-case basis.

(b) The Information Request Form allows a requester to complete certain information – their identity, purpose of the request and the DPPA exemption which allows them access – in order to obtain an unredacted record containing DPPA-protected information. For example,

Section I of the Form contains the requester's information. Section II asks for information about the request. Section III contains a list of the DPPA's exemptions to be selected by the requester. Sections IV and V contain penalties and certifications.

(c) As an example, such as might come from a media representative, the release of an unredacted record will be contingent upon the record requester completing the Form indicating that the use of the information satisfied the DPPA exemption found in Section III sub. 14, that the "use is related to the operation of a motor vehicle or public safety." Thus, an acceptable response in completing Section II in some instances would be citing the exemption found in Section III sub. 14.

Title 6 ▸ Chapter 3

Juvenile Records

Sec. 6-3-1 General Principles and Definitions.

DEFINITIONS:

The following definitions and principles shall be applicable in this Chapter:

(a) **Authority.** Any law enforcement agency Clark or Chippewa Counties; a County Department of Health and Human Services; any office representing the interests of the public in Clark and Chippewa Counties under Sec. 938.09, Wis. Stats.; any municipal court in Clark or Chippewa Counties exercising jurisdiction under Sec. 938.17(2), Wis. Stats.; any person, office or social welfare agency providing legal defense, guardian ad litem, investigative, intake, assessment or dispositional services (including informal dispositions and consent decrees) for children or other subject to the jurisdiction of the Clark or Chippewa County Juvenile Court.

(b) **Balancing of Interest.**

(1) It is not uncommon that one party's interest in having a record disclosed is opposed by another party's interest in having the record remain confidential. The statutes do not, however, provide much guidance as to how the decision whether to disclose should be made. In general, this decision is left to the discretion of the custodian of the record or the juvenile court judge.

(2) The Wisconsin Supreme Court has provided some guidance in the *Herget* decision which has been codified at Sec. 938.396(5), Wis. Stats. While the use of these criteria is limited to access to law enforcement records in connection with civil litigation, they are useful in other disclosure situations. While the application of the criteria are not required by law in those other situations, these policies adapt and apply them, whenever possible, in order to meet the Judge's interpretation of the intent of the law.

(c) **Confidentiality.**

(1) This means that a record or other communication may not be disclosed to a person or entity which is not authorized by law to see or hear it. It is not a right; a person may neither claim nor waive confidentiality. Rather, it is a status which is controlled by statute.

(2) A related concept is "continuing confidentiality." This means that the lawful disclosure of a confidential item to a third party does not result in the item losing its confidential status. The person who received the confidential item may not further disclose the item unless authorized by law to do so. The only exception to this rule is when the authorized use of the confidential item results in lawful public disclosure, eg., a person's juvenile court record contained in an adult pre-sentence report, or a civil action filed by a victim of a juvenile offender's act.

(d) **Confidential Record.** A record which may not be disclosed, except by an appropriate court order, through a statutorily authorized exchange which assures the continuing confidentiality of the record, or by a person exercising a statutorily authorized privilege.

(e) **County Department.** The Clark or Chippewa County Department of Health and Human Services.

(f) **Court.** The circuit court assigned to exercise jurisdiction under Chs. 48 or 938, Wis. Stats.

(g) **Juvenile Court Record.** All records under the control of the Clerk of Court pursuant to Sec. 59.39, Wis. Stats., any record made pursuant to juvenile court order (including, but not limited to, examinations under Sec. 938.295, Wis. Stats., consent decrees under Sec. 938.32, Wis. Stats., court reports under Sec. 938.33, Wis. Stats., and dispositional records) and records of intake relating to custody intake under Sec. 938.20(3), Wis. Stats., and referrals made pursuant to Sec. 938.24, Wis. Stats.

(h) **Law Enforcement Record.** Any record under the direct control of a law enforcement agency.

(i) **Mental Health Record.** Any record which is subject to the provisions of Sec. 51.30, Wis. Stats., or 42 C.F.R. Part 2.

(j) **Open (or Public) Records Law.** Wisconsin has a relatively strong public policy assuring the public's right to access and have disclosed "information regarding the affairs of government and the official acts of those officers and employees who represent them" (Sec. 19.31, Wis. Stats). The public's right in this regard is absolute, "except as otherwise provided by law" (Sec. 19.35, Wis. Stats.). Thus, confidentiality required by statute takes precedence over the public's right of access.

(k) **Privilege.**

(1) This concept extends the right to privacy to certain communications which otherwise might be lawfully admitted into evidence at a trial. The individual possessing the privilege has the right to refuse to disclose and to prevent any other person from disclosing certain confidential communications, and in the converse, must formally approve such disclosure. Generally, those communications between a person and his or her lawyer, physician, nurse, chiropractor, psychologist, spouse and clergyperson are privileged. Privilege is not absolute, however. The Wisconsin rule of privilege and exceptions to the rule are detailed in Ch. 905, Wis. Stats. Two privileges for students are provided at Secs. 118.126(1) and 885.205, Wis. Stats.; however, the former is limited. Only those privileges specifically stated in state statute are recognized in Wisconsin; Wisconsin does not recognize common law privileges (*Davidson v. St. Paul & Marine Ins. Co.,* 75 Wis.2d 190).

(2) Communications made to social workers, juvenile court intake workers, and dispositional staff are not privileged.

(l) **Privileged Record.** A confidential record which may be disclosed or prevented from being disclosed by an individual who may claim a statutorily authorized right to take either action.

(m) **Record.** Any material on which written, drawn, printed, spoken, visual or electromagnetic information relating to a juvenile is recorded or preserved, regardless of physical form or characteristics which has been created or is being kept by an authority, but does not include notes prepared for personal use by the creator of the record, information relating to a juvenile within the exclusive jurisdiction of a court which does not exercise jurisdiction under Chs. 48 or 938, Wis. Stats., or as otherwise excepted by these policies.

(n) **Reporters of News.** Any person employed by an organization regularly disseminating news to the public.

(o) **Reporting Act Record.** Any document relating to the investigation, assessment and determination of a child abuse or neglect report made pursuant to Sec. 938.981(3), Wis. Stats., and subject to the provisions of Sec. 938.981(7), Wis. Stats.

(p) **Right to Privacy.** In its most simple form, the right to privacy means that each citizen has the right to be left alone and free from government intrusion into his or her private life except as specifically provided by law. In Wisconsin, this right is recognized by statute (Sec. 895.50, Wis. Stats.).

(q) **Social Services Record.** Any record under the direct control of the County Department of Health and Human Services or of a social welfare agency providing services to either the county department or the juvenile court containing information about an individual who has been referred to or is receiving services from either the county department or agency.

County Health and Human Services Department records affected by this policy are those that are related to Chs. 48 or 938, Wis. Stats.

(r) **Social Welfare Agency.** Any agency or facility licensed or authorized under Chs. 48 or 938, Wis. Stats., any agency or organization providing social or diagnostic services to the juvenile court or the county department, any other human services agency formally recognized by the juvenile court.

COMMENTARY:

It is declared policy in Wisconsin that the public shall have complete access to all governmental records, including those of the state's circuit courts. Denial of public access is the exception. This policy is consistent with our form of government and deserves the vigorous support of all government officials.

The legislature has created and maintained a limited number of exceptions to this general policy of complete public access. Most public records concerning children have historically been shielded from public view. While limited public access is occasionally permitted, the general public policy has been to keep these records confidential with disclosure being the exception. In upholding the Legislature's decision to close law enforcement, social agency and court records relating to children, the Wisconsin Supreme Court set forth a clear rationale for this relatively exceptional policy:

> Confidentiality is essential to the goal of rehabilitation, which is in turn the major purpose of the separate juvenile justice system. In theory, the role of the juvenile court is not to determine guilt or to assign fault, but to diagnose the cause of the child's problems and help resolve those problems. The juvenile court operates on a "family" rather than a "due process" model. Confidentiality is promised to encourage the juvenile, parents, social workers and others to furnish information which they might not otherwise disclose in an admittedly adversary or open proceeding. Confidentiality also reduces the stigma to the youth resulting from a misdeed, an arrest record and a juvenile court adjudication.
>
> *State ex rel. Herget v. Waukesha County Circuit Court*
> 84 Wis.2d 435, 267 N.W.2d 309, 316 (1978).

The Children's Code and related statutes specifically provide for the confidentiality of certain sets of records, but with few exceptions do not define in any clear way what these sets of records include.

Prior to the creation of the Children's Code in 1955, not all of the records relating to juveniles were confidential. Police records, for example, were open while the juvenile court record, which

contained much the same information as the police record, was closed. According to the legislative history of the 1955 Children's Code revision (which required confidentiality much as we know it today), "[t]he result is that in some cases the purpose of requiring the other records to be closed is lost." (1955 Wisconsin Legislative Council, Vol VI, Part I, Conclusions and Recommendations of the Child Welfare Committee, p. 29).

While the legislature has declined to specifically define, for example, a "court record" or a "social services record," it has since 1955 continued to recognize these separate sets of records. Sec. 938.396, Wis. Stats., addresses both "peace officer's" records and "court" records; Sec. 938.78, Wis. Stats., addresses "agency" records, which includes the records of a county department. Therefore, courts must provide the necessary meanings so as to allow the statutes to operate in a meaningful, coherent fashion as intended by the legislature.

Three principles guided the development of the definitions detailed above. First, the general rule in the juvenile court and social services systems is that records relating to children are confidential; that is, their contents shall not be disclosed without court order. Disclosure without court order is the exception and should occur infrequently, either through a statutorily authorized exchange, when an individual exercises a statutorily authorized privilege, or when permitted by court policy.

Second, there must be a legitimate distinction between types of records if the words of the statutes are to be given meaning. For example, if all the court's records, eg., petitions, findings and orders, are replicated in the child's social services record and subject to exchange under Sec. 938.78, Wis. Stats., does not the court lose control over the disclosure of its records, in effect obviating the legislative intent of Sec. 938.396(2), Wis. Stats., in much the same manner as was the case with police records prior to 1955? The presumption must be that most of the records in a juvenile's case, from intake through termination of the case, are court records [see *State ex rel. S.M.O. v. Resheske,* 110 Wis.2d 447, 453 (CA 1982)]. The court is aware that this principle could create a few practical problems and has sought to achieve a consensus of definition among affected agencies.

Third, a record could meet more than one definition at any given point in time. This is to be expected given the near impossibility of physically re-classifying each record within each agency each time the record moves through different agencies and parts of the system. The specific policies on access and disclosure which follow will define the hierarchy of records and the appropriate procedures to be utilized in any given instance.

Sec. 6-3-2 Law Enforcement Juvenile Records.

POLICY:

(a) **Maintenance and Access.** The juvenile records of the Police Department shall be kept separate from those of adults and shall be confidential. Access to and disclosure of such

records shall only be made upon written order of the juvenile court, except as follows [Sec. 938.396(1), Wis. Stats.]:

[All requests and orders for records under Subsections (a)(2) and (3) below must be entered and maintained in the subject's law enforcement file. Releases of information under Subsections (a)(5) and (6) below, and the name of the individual to whom it was released, must be noted in the subject's file. Such requests for information shall be in writing].

(1) ***Parents, Guardians, Legal Guardians or Juveniles Age 14 or Over.***
   a. Upon request of parent, guardian or legal custodian or juvenile, age fourteen (14) or over, a copy of the law enforcement report may be given to them, subject to official agency policy. [Sec. 938.396(1b), Wis. Stats.]
   b. Upon written permission of the parent, guardian, legal custodian or juvenile, age fourteen (14) or over, specifically identified reports may be made available to the person named in the permission, subject to official agency policy. [Sec. 938.396(1d), Wis. Stats.]
   c. If a law enforcement agency discloses information, it must immediately notify the juvenile who is the subject of the record and the juvenile's parent, guardian or a legal custodian and shall immediately provide to them the information disclosed. [Sec. 938.396(v), Wis. Stats.]

(2) ***Reporters of News.*** Reporters of news shall have access without court order, but shall not reveal the identity of the child involved. There is not an absolute prohibition regarding the publication of a child's identity if that information is received from a private source. It is hoped that the media will continue to respect the policy of non-identification in the interest of children and families.

(3) ***Prosecutors.*** The appropriate representative of the public under Sec. 938.09, Wis. Stats. (most commonly, but not limited to, the District Attorney or corporation counsel), shall be given all records necessary for the prosecution of all cases under Chs. 48 and 938, Wis. Stats., and shall be given specified records in response to a request for discovery under Sec. 938.293, Wis. Stats. The identity of a confidential informant may be withheld as provided in Sec. 905.10, Wis. Stats. Discovery requests made to law enforcement by a party or their counsel should be denied and referred to the prosecutor. Law enforcement officials must comply with discovery orders issued by the court.

(4) ***Victims.***
   a. Victim–witness coordinators have access to law enforcement records under Sec. 938.396(1),(1g), Wis. Stats.
   b. Victims can request information on injury, loss or damage, including name and address of the juvenile and parents. [Sec. 938.396(1r), Wis. Stats.]
   c. A victim's insurer may request information on injury, loss or damages, including name and address of the juvenile and parents, if the juvenile fails to make court

ordered restitution within one (1) year after the order is entered. [Sec. 938.396(1t), Wis. Stats.]

d. The judge of the juvenile court may order the disclosure of specified records for use in a civil action against a child or his/her parents under Sec. 938.396(5), Wis. Stats. In such an instance, disclosure is limited to those specific records or portions thereof specified in the court's order and shall be transmitted in a manner which assures the continued confidentiality of the records.

(5) ***School Officials.*** School districts can request information from police records relating to the act for which a juvenile enrolled in the public school district was adjudged delinquent. [Sec. 938.396(1m)(b), Wis. Stats.] School use is limited by Sec. 118.127(3), Wis. Stats. Information contained in a record concerning a student of a public or private school may, at the Police Department's discretion, be given to the designated custodian of the records of the school attended by the student, but only if the Department is assured that the confidentiality of the information will be absolutely maintained by the school official receiving it and used only for those specific purposes agreed to by the Department and the school. Such information in the school file must be marked confidential and retains its law enforcement record status.

For further information the following excerpt is taken from "Confidentiality and Juvenile Records" by Peter Plant, Juris Press 1987, pg 12-13:

> "This issue has been the subject of two Attorney General's Opinions. The first, 69 OAG 179, was issued in 1980. After stating that a juvenile officer is not required to provide this information, the Attorney General held that a school could theoretically use the information to take disciplinary action against the student, but only "if the confidentiality of that information is properly preserved by school officials." However, since it is highly unlikely that such information could be used without disclosing it to persons not authorized to receive it, the circumstances which would allow its use are very limited since most major disciplinary actions are subject to hearing and review procedures involving many other officials. The Attorney General cautioned law enforcement officials not to disclose such information "when there is reason to believe that the information sought will not or could not practically be kept confidential" as required by law. If the office or agency does provide the information, it may only be used for purposes previously agreed to be the officer or agency."
>
> "A more recent Opinion (OAG 30-87; June 12, 1987) has expanded on the one described above. In this instance, the questions posed by school officials related to whether information

received from law enforcement could be used for both disciplinary and referral purposes. The Attorney General's view was emphatically stated:

> In my opinion, a school cannot use confidential information obtained from the police to require students, under the threat of expulsion, to participate in group or individual counseling, nor can the school use such information to suspend or expel students.

"The information may be used to refer the student to helping services, but only if the student consents to the referral."

"The 1980 Opinion recommended that if school officials wished to use the information for any purpose which might result in further disclosure, they should request a court order from the juvenile court judge to do so. This authority had been provided for in Sec. 938.396(1), Wis. Stats. A technical amendment to 1987 Wisconsin Act 27 (the budget bill), however, inadvertently repealed this authority. As presently written, the statute now only allows the juvenile court judge to order disclosure of law enforcement records pursuant to request for discovery (Sec. 938.293, Wis. Stats.), and from the victims of the juvenile's acts [Sec. 938.396(5), Wis. Stats.]. Although this repeal does not appear to be intentional, it is nevertheless law until changed. Thus, the historical option available to all others, including school officials, to access these records no longer exists."

(6) ***Other Agencies.*** The Police Department may choose to share its records, portions thereof or information contained in a record with other law enforcement agencies, the County Health and Human Services Department or with social welfare agencies the Department recognizes, but only if the Department is assured that the confidentiality of the record or information will be maintained by the party receiving it.

NOTE: Child abuse or neglect law enforcement records are controlled by Sec. 938.981(7), Wis. Stats.

(b) **Denial of Access.** Any request for a record or information which does not come within one of the exceptions, above, shall not be granted, even if the requesting party presents a waiver of confidentiality for the record signed by the juvenile subject or parent. The

Department shall respond that state law prohibits a response to the inquiry (56 OAG 211) and that the requesting party or the juvenile subject agreeing to disclosure may wish to contact the juvenile court for further information or assistance in obtaining a court order for access and disclosure.

Any party denied access under Subsection (a)(4) or (5) above may seek a court order for access.

(c) **Notice of Continuing Confidentiality.** Any person receiving a record whether by exception or court order shall be given notice that the record or information disclosed continues to be a Department record and shall be kept confidential and used only for purposes authorized by statute or approved by the court. A reporter of news who discloses the identity of a juvenile may be subject to Sec. 939.61, Wis. Stats.; any other person disclosing such records or information without lawful authority may be subject to contempt of court or other civil action.

The notice provision of this Subsection does not apply to law enforcement agencies, employees of the County Health and Human Services Department, representative of the public under Sec. 938.09, Wis. Stats., or counsel or guardian ad litem for the child or parent, who are presumed to know and comply with the confidentiality provisions of Wisconsin law.

(d) **Records Excepted.** This policy does not apply to records relating to an offense or incident for which the child has been waived to the criminal courts under Sec. 938.18, Wis. Stats.; certain civil law and ordinance matters subject to adult court jurisdiction under Sec. 938.17(1) or (3), Wis. Stats.; or references to children who are not the subject of any formal or informal action under Chs. 48 or 938, Wis. Stats., eg., a witness, passenger in a vehicle, or a bystander.

Title 6 ▸ Chapter 4

Computing Value of Lost/Stolen Property

Sec. 6-4-1 Guidelines for Computing the Value of Property Stolen/Recovered.

PROCEDURES:

(a) Determining the value of property is often a difficult problem. It is essential that the investigating officer ascertain and include values in the preliminary report.

(b) Use fair market value for articles which are subject to depreciation because of wear, age or other factors which cause the value to decrease [for instance, a pair of men's shoes purchased for Fifty Dollars ($50.00) three (3) years prior to their being stolen might only have a fair market value of Five Dollars ($5.00) at the time of theft].

(c) Use cost to the merchant for goods stolen from retail establishments, warehouses, etc. If the retail cost is used, a notation shall be made in the narrative.

(d) Use the victim's valuation for items such as jewelry, watches, etc., which decrease in value only slightly with use or age.

(e) Use replacement cost or actual cash cost to victim for new or almost new clothes, auto accessories, bicycles, etc.

(f) Use professionally appraised value, if available, for collections of coins, stamps, art objects, antiques, etc.

(g) When the victim obviously exaggerates the value of stolen property, your own common sense and good judgment should dictate a fair value. In most cases, the victim's valuation can probably be accepted, subject to the above guidelines.

(h) Non-negotiable instruments, such as travelers' checks, personal checks, money orders, stocks and bonds, etc., should be classified according to appropriate offense if stolen, but no value should be recorded.

(i) Negotiable instruments, such as bonds "payable to bearer", checks made out to cash (not endorsed), etc., capable of being passed without committing the offense of forgery, should be recorded at face value of fair market price at the time of theft.

(j) Recovered property may be in a condition other than when it was stolen, with a consequent decrease in value. Record the value at time of recovery, even if less than stolen.

(k) Recovered property, such as coins and art objects, may have increased in value from time of loss to time of recovery. Record the value at time of recovery, even if greater than when stolen.

(l) Restitution does not constitute "recovered" property.

Title 6 ▸ Chapter 5

TIME System

Sec. 6-5-1 System Security.

POLICY:

Each City of Stanley Police Department employee is responsible for allowing only authorized personnel to operate the TIME terminal, and enforce system and data security. As a part of this responsibility each employee is responsible for insuring that the terminal is used for authorized and official messages only.

Sec. 6-5-2 Data Security.

POLICY:

Data stored in central repositories such as CIB (Crime Information Bureau) and NCIC (National Crime Information Center) files which are a part of the TIME System must be protected from unauthorized access and restricted to authorized law enforcement agencies. This Department

accesses TIME System files, but is not custodian of those records. Any request for release of records shall be made to the custodian of those records, (i.e. DOT, CIB) and not the user of those records.

Sec. 6-5-3 NLETS (National Law Enforcement Telecommunications System) Policies.

PROCEDURES:

(a) When this agency requests CHRI (Criminal History Record Information), it shall ensure that proper controls are established such that only authorized criminal justice agencies and personnel can access CHRI.

(b) Authorized personnel having access to the TIME System shall utilize specific transaction screens for CHRI requests.

(c) All personnel shall adhere to the approved operational procedures required for responding to CHRI requests.

(d) Requests for CHRI, and responses to requests for CHRI by authorized criminal justice agencies and personnel are for legitimate purposes.

(e) All authorized CHRI message requests shall receive a response.

(f) Personnel requesting CHRI or responding to requests for CHRI shall comply with the US Department of Justice Rules and Regulations as they relate to completeness, accuracy and the dissemination of CHRI.

(g) Personnel shall comply with the policies and procedures for the interstate exchange of CHRI as set forth in the TIME System Policies.

Sec. 6-5-4 Department of Transportation Records.

POLICY:

(a) **Generally.** The Wisconsin Department of Transportation (DOT) is the custodial agency of vehicle and driver record files, and dissemination of information is the responsibility of the custodial agency.

(b) **Vehicle Registration Files.**

(1) TIME System agencies are not obligated to furnish registration information obtained from the Department of Transportation via their TIME terminal.

(2) Public requests for registration information should be referred to:

Wisconsin Department of Transportation
Vehicle Registration Files
P.O. Box 7909
Madison, WI 53707 Telephone: (608) 266-1466

(3) The same guidelines used for vehicle registration applies to other registration information available on the TIME System, such as boats, snowmobiles and aircraft. This department is not the custodian of those records and therefore will not release those records to the public.

(4) Likewise, information as to whether or not the vehicle or item queried through the TIME System is wanted or stolen will not be released, however, it may be broadcast in the interest of officer safety.

(c) **Driver Information Fields.**

(1) The City of Stanley Police Department will advise any person requesting a driver abstract to contact DOT by mail. The address is:

Wisconsin Department of Transportation
Driver Record File
P.O. Box 7918
Madison, WI 53707 Telephone: (608) 266-1466

(2) Warrant/wanted or missing status will also not be released unless such release complies with TIME regulations. These records are the property of the entering agency and the TIME System.

Sec. 6-5-5 Juvenile Department of Transportation Record Information.

POLICY:

(a) Sec. 343.24(3), Wis. Stats., pertains to dissemination of juvenile records maintained by the Department of Transportation. This Statute states the Department shall not disclose information concerning or related to these violations to any person other than a court, district attorney, county corporation counsel, city, village or town attorney, law enforcement agency, the minor who committed the violation, or their parent/legal guardian.

(b) Since this information is present on driver record checks made by law enforcement agencies, it is necessary that it not be divulged to anyone and is to be used for the internal use of this Department or the above listed officials.

PROCEDURES:

(a) These entries will always be listed as "confidential".
(b) These entries include but are not limited to:
  (1) JA—Juvenile alcohol.
  (2) FPJ—Fail to pay juvenile forfeiture.
  (3) T–Truancy.
(c) These entries must remain confidential and should therefore not be released or broadcast on an open radio frequency, unless for some reason there is an entry that involves officer safety.
(d) In determining juvenile enteries for penalties/bonds, officers should utilize their laptop computers and should not broadcast juvenile names over the radio.

Sec. 6-5-6 Criminal History Record Information.

POLICY:

(a) **Criminal History Record Information.** (CHRI) means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrest, detentions, indictments, information or other formal criminal charges and any disposition arising therefrom, sentencing, correctional supervision and release. (Department of Justice Rules and Regulations on Criminal Justice Information Systems 41 Federal Regulations 11714, 03/19/76).

(b) **Privacy Considerations.**

  (1) The following abbreviations shall be applicable herein:
    a. C: Criminal.
    b. J: Justice Employment.
    c. E: Employment.
  (2) CHRI must be afforded strict privacy considerations by law enforcement agencies. Requests for CHRI must be submitted in the proper format utilizing the proper purpose codes to ensure prohibited information is not released to unauthorized persons.
  (2) Purpose Codes C and J may be used for official criminal justice inquiries. They may be used for CIB inquiries and III (Interstate Identification Index) inquiries, and inquiries to other states.
  (3) Purpose Code E may be used only for CIB inquiries. This code is to be used only for specific administrative and statutory licensing, regulation or permit responsibilities of the City of Stanley. Purpose Code E will result in the City being billed by CIB for the inquiry. *No other purpose may be used when performing a CHRI check for the purpose of licensing.* III will not accept Purpose Code E, and no other legitimate purpose code may be used to bypass the built in safeguards preventing use of III

information in licensing. Purpose Code J can be used for queries for Criminal Justice Employment Purposes (background or pre-employment checks.)

(4) a. Individuals requesting a copy of their record from CIB may do so by contacting CIB in writing. Persons requesting access to a copy of their record from the FBI (III) may do so by contacting the FBI in writing, along with a set of rolled fingerprint impressions and prepayment of the required fee.

b. The Wisconsin Open Records Law provides for public access to CHRI records maintained by CIB, unless the record is specifically exempted by law. (Juvenile release is specifically exempted).

(5) As CHRI records released by CIB to law enforcement agencies via the TIME System become a local agency record and subject to release under the open records law, and may not necessarily be up to date and accurate when the request for information from the case is made, CHRI records will not be maintained in case files. Identifiers obtained from CIB may be maintained in the record, but the actual criminal record will be disposed of once the case has been forwarded to the prosecuting attorney or, if not forwarded, when the case is closed.

(6) CHRI records obtained through III are exempt from disclosure under the Open Records Law based on the Privacy Act of 1974. The Privacy Act of 1974 also provides criminal penalty for:

a. Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses.

b. Any employee entitled to criminal history information who obtains such information from the FBI with the intention of using it for an unauthorized purpose,

c. An individual who knows that he/she has no right to such information, and who, under false pretenses, receives the information from the above-described employee, or,

d. Any person who knowingly receives, under false pretenses, criminal history record information via an unauthorized request directed to the FBI.

Sec. 6-5-7 Physical Security.

POLICY:

The TIME System terminal must be placed in a location that is not available to the general public. Unauthorized personnel are not to have access to the data from either the terminal display or printer. The TIME System has various built-in security measures, but final responsibility for physical security rests with the terminal location agency.

Sec. 6-5-8 TIME System Training.

POLICY:

(a) **NCIC Policy Requires That the State:**

(1) Ensure that the appropriate Communications Center (terminal agency) designate an employee to function as a Terminal Agency Coordinator (TAC) who shall be responsible for ensuring compliance with the State and NCIC policy and regulations to include terminal operation and validation requirements.
(2) Initially train, functionally test and affirm the proficiency of terminal operators in order to assure compliance with NCIC policy and regulations.

(b) To comply with the above stated guidelines, this Department strives to meet the following guidelines:

(1) Certify all Police Telecommunicators in the six (6) month NCIC guidelines.
(2) Train all sworn or clerical personnel who operate the TIME terminal in relief or in lieu of a Telecommunicator.
(3) Once certified, all operators will maintain their certification.
(4) Those employees who allow their certification to lapse will be recertified.
(5) All TIME terminal users shall at a minimum read and complete the New Operator Training handout, which shall be retained by the TAC until submitted for operator training.
(6) Once certification has been completed, only certified TIME System Operators will serve as primary operators.
(7) All operators will keep up-to-date on any TIME System changes by reading the TIME System Newsletters published by the State of Wisconsin CIB.

Sec. 6-5-9 TIME System Data File Entries.

POLICY:

(a) **Documentation Required for Entry.** Entry of data in the TIME System can only be accomplished if the agency has proper documentation in its possession. Examples of suitable documentation for the various files are listed as follows:

(1) ***Wanted Person File.*** Must possess a court issued warrant. Any warrant will contain an extradition forecast indicated whether or not they will extradite, and what geographical restrictions are placed on that extradition.
(2) ***Missing Person File.***
a. Must possess signed documentation from a source outside the Department supporting the conditions under which the person is declared missing. Examples are:

1. Signed missing person form or written statement from parent/legal guardian confirming that the person is missing and verifying all possible physical/mental disability;
2. Written statement from a physician or other authoritative source corroborating the missing person's physical/mental disability;
3. Written statement from parent, legal guardian, family member of other authoritative source advising that the missing person's disappearance was not voluntary or that the person is in the company of another person under circumstances indicating that the missing person's physical safety is in danger.
4. The National Child Search Assistance Act of 1990 requires that agencies verify and update original NCIC missing juvenile entries with any additional information, including medical and dental records, within thirty (30) to sixty (60) days of entry.
5. NCIC will automatically review missing and unidentified person entries to determine if information is present in the blood type, dental characteristics, fingerprint classification, jewelry type, scars, marks, tattoos and other characteristics fields.
6. If one (1) or more of the above fields is missing data, an online $.K Message will be sent to the entering agency between 0630 and 0730 CST.
7. The $.K Message should serve as a reminder to make contact with the source of a missing or unidentified entry to determine what additional information can be added to the entry. If the entry is modified or supplemented in any way, the entry will again be searched against other missing or unidentified entries. (Refer to NCIC Security Log for $. message information.)

(3) ***Property Files.***

a. Must have an investigative report stating that the property (vehicle or part, article, boat or part, gun or security) was taken without consent of the owner or custodian of the property.
b. Persons reporting missing property that has been entered into the TIME System shall be contacted again within sixty (60) days of the date of entry to check on the current status of the property, as to whether or not it has been recovered/located by the reporting person, or as to any additional identifiers for the property the reporting person may have information on.
c. Procedures require that all guns recovered that have not been reported as stolen be entered into the Recovered Gun File.

(4) ***Stolen Registration Plates.*** No registration plate will be entered in the System until verification that registration was canceled by DOT. Individuals losing a registration plate should be advised to contact DOT and have registration canceled and notify this department of the cancellation by DOT and remove matching plate from the vehicle

as well. Individuals may be directed to the Wisconsin Department of Transportation Form MV2514 License Plates Cancellation Application.

(5) ***Violent Gang and Terrorists Organizations File.***

a. The Violent Gang and Terrorist Organization File (VGTOF) is designed to provide law enforcement personnel with identifying information about violent criminal gangs and terrorist organizations and the members of those groups. This information warns law enforcement officers of the potential danger posed by violent individuals. The file should also promote the exchange of information about these organizations and their members to facilitate criminal investigations.

b. VGTOF information is based, in part, on investigative information that has not been subject to an independent judicial review. For that reason, strict adherence to the NCIC policy on the security, use and dissemination of VGTOF information is necessary.

c. Violent gang and terrorist organization information is exclusively for the use of criminal justice agencies for criminal justice purposes. VGTOF information should *never* be disseminated to any non-criminal justice agency. The same security measures used when dealing with Interstate Identification Index (III) criminal history records should be exercised when receiving information from this file.

d. The VGTOF contains two (2) components which were designed to accomplish two (2) major goals: promoting the identification of groups and group members and facilitating the exchange of information about these groups and members:

1. The *Group Member Capability (GMC)* provides information about individual members of gangs or terrorist organizations. The VGTOF will be searched on every person query. The response will be returned in a format similar to an NCIC wanted person record. Law enforcement agencies are able to make individual entries of gang members. Information regarding the accuracy of a group or individual record must be available during an audit.
2. The *Group Reference Capability (GRC)* provides information about gangs or terrorist organizations. Prior to making a group entry, a law enforcement agency must complete a Group Registration Form and submit the form to CIB. The Crime Information Bureau forwards this document to NCIC which, in turn, assigns a group code. This code is necessary for entry.

e. NCIC has developed guidelines that should be reviewed prior to completion of a Group Registration Form.

f. To qualify for entry, a *"Gang"* must meet the following criteria:

1. Must be an ongoing organization, association, or group of three (3) or more persons; and
2. Must have a common interest and/or activity characterized by the commission of or involvement in a pattern of criminal or delinquent conduct.

g. A *"Terrorist Organization"* must meet the following definition:
   1. Must be an ongoing organization, association, or group of three (3) or more persons; and
   2. Must be engaged in conduct or a pattern of conduct which involves the use of force or violence; and
   3. The purpose of the group in using violence must be to intimidate or coerce a government, civilian population, or segment thereof, in furtherance of political or social objectives.

h. Criminal activities or delinquent conduct includes activities such as murder, extortion, firearms or explosives violations, assault and burglary. Groups whose only activity is spray painting, i.e. taggers, do not qualify for entry.

(6) ***Deported Felon File.***

a. The Immigration and Naturalization Service (INS) maintains the NCIC Deported Felon File. They are the only agency authorized to enter or update records. Before the INS will enter a record, an alien must meet the following criteria:
   1. Be a convicted felon who has been deported for drug trafficking, firearms trafficking, or another serious violent crime.
   2. Be a citizen and/or national of a contiguous territory or an adjacent island.

b. The Deported Felon File will be searched on every person query. NCIC will attach caveats to the response to distinguish a deported felon record from a wanted person record. *The caveat before the record warns the receiving agency not to take action based on the positive response alone. A second caveat, placed at the end of the record, indicates that the information contained in the record is to be used by criminal justice agencies for criminal justice purposes only.*

c. An officer who receives a positive response from the Deported Felon File should proceed as follows:
   1. If the inquiry was made under routine circumstances, such as a traffic stop, the individual should not be detained, based solely on this notification. If the officer has no other reason for detaining the individual, he or she should get all pertinent data relating to the individual and forward the information to the INS via administrative message. Pertinent information includes subject's address, vehicle and license information, and any other identifying information, such as social security number.
   2. If the individual is arrested or detained on other charges, the arresting agency should notify the INS Command Center at 202/616-5000 to confirm the identity of the subject. Once the INS is notified that a deported felon has returned to the United States, they will send INS personnel to interview the subject. If the criminal alien has not received permission to return, the INS and U.S. Attorney's Office will begin prosecution.

(7) ***Orders and Injunctions File.***

a. Wisconsin law enforcement agencies must report restraining orders and injunctions to the Department of Justice. Agencies will be able to do this on-line

via the TIME System's Orders and Injunctions File (OIF). This file will contain information on persons who have had either a temporary restraining order or an injunction issued against them. Initially, there will be eight (8) categories for entry:

1. Temporary Restraining Order—Domestic Abuse.
2. Temporary Restraining Order—Child Abuse.
3. Temporary Restraining Order—Harassment.
4. Injunction—Domestic Abuse.
5. Injunction—Child Abuse.
6. Injunction—Harassment—Firearms prohibited.
7. Injunction—Harassment—Firearms not prohibited.
8. Other.

b. Because a restraining order or injunction is issued only after a serious situation has come to the attention of the court, it is important that information on injunctions and restraining orders be entered into the TIME System as soon as possible. Law enforcement agencies will be able to query this file when responding to domestic violence calls. The additional information provided through the file response could affect the way the officer handles the call.

c. Wisconsin law also prohibits some persons who are affected by an injunction from possession a firearm. The OIF file will be checked whenever a person attempts to purchase a handgun. If DOJ's Handgun Hotline staff finds that an injunction is on file, they will deny the transfer of a handgun.

(8) ***CIB Detainer File.***

a. Implementation of a Detainer File will allow an originating agency to append detainer information to an existing warrant/wanted person record until the subject's sentence is served at another agency and arrangements for pickup can be made. Creation of this file should preclude the release of a person wanted by other agencies.

b. A detainer worksheet may be placed when hit confirmation has occurred and the arrested subject will not be released to the agency holding the warrant until local charges have been satisfied. If the warrant is in CIB only, the detainer worksheet can be appended to the already existing record. If the warrant is in both CIB and NCIC, the record must be cancelled and re-entered into CIB only. This is due to NCIC's policy stating records *must* be cancelled after hit confirmation has occurred. Once the record is re-entered into CIB, the detainer worksheet can be appended to it. The required fields for placing a detainer are: Date of Detainer, Incarcerating Agency, Date Incarceration Starts, Date Sentence Ends, Place of Incarceration and Remarks.

c. If Subsection (a)(8)b is not utilized, officers shall cancel the warrant and place the detainer by using an "administrative message". This administrative message shall be sent by the terminal agency.

(9) ***National Insurance Crime Bureau Files.***

a. The National Crime Insurance Bureau, formerly known as the National Auto Theft Bureau (NATB), maintains a rapidly expanding national and international index of vehicle records. This includes information about manufacturer's shopping and assembly, vehicles imported and exported, thefts, impounds, salvage, auction, pre-inspection, vehicle claim and rental. To track a motor vehicle's complete life cycle from manufacture to demolition, the NICB data base is designed to include vehicle, liability, physical damage, and related homeowner claims. NICB files include data on passenger vehicles, multipurpose vehicles, trucks, trailers, motorcycles, snowmobiles, construction and farm equipment, boats, and uniquely identifiable parts.

b. The Insurance Bureau provides automated access to nine (9) different files:
   1. Manufacturers' Shipping;
   2. Impound;
   3. Export;
   4. Salvage;
   5. Auction;
   6. Pre-Inspection;
   7. Vehicle Claims;
   8. Rental; and
   9. International Index.

   TIME System users will be able to query these files as well as add vehicles to the impounded file.

c. There are two (2) NICB inquiry transactions. One will access only the Impound and Export files while the other will access all nine files maintained by the Bureau. The NICB files are to be used for investigative purposes only. These files will *not* be searched during a routine vehicle query. The Impound/Export File inquiry examines the NICB Impound and Export files only. An impound record will be returned only if the vehicle was seized within the previous sixty (60) days.

d. NICB has some special requirements for querying a vehicle identification number. If only a partial VIN is available the user may submit either the last eight (8) characters of the VIN or the last 6 and the 2 character year. In order to identify the VIN as partial to NICB the user *must* preface the partial VIN by the word "PARTIAL" and end the search with the year of manufacture.

e. For example, a partial VIN from a 1990 vehicle would be entered as: PARTIAL24654790. Note that there is no space between the word "PARTIAL" and the six (6) character VIN or the year of the vehicle. When a query using a partial VIN is made, *only the Manufacturers Shipping File will be searched.*

f. If no information is found on any of the nine (9) NICB files a "NO RECORD NICB" message will be received.

(b) **When to Make Data File Entry.** Entry into the data files should be made immediately upon receipt of required documentation and minimum data required for entry.

(c) **Data Requirements.**

(1) Although data entries may be made with minimum data, it is the policy of this Department to enter as much information as is available. If data becomes available at a later date, the record may be modified or supplemented to include the new information.

(2) Inquiries must be made through both the TIME System and the Department's in-house computer system to obtain all the data available. Any new information obtained via the TIME System should be retained in the case jacket to show where the identifiers were obtained from, and may be incorporated into the in-house system at a later date. Any information that cannot be verified will not be included in the data entry.

(d) **Data Entry Quality Control.** In an effort to make sure data entry files do not contain errors, it is the policy of this Department to have the data entered by one (1) certified TIME System operator and checked by another whenever possible.

Sec. 6-5-10 Validation Procedure.

POLICY:

(a) No records entered by this Department into the CIB/NCIC files will be validated without verification from the person or official responsible for the initial report, or from someone who has assumed responsibility for the record/property (i.e. Chief of Police and/or TAC Officer).

(b) Verification of warrants/wanted persons, missing persons or unidentified persons shall be done by the Chief of Police and/or TAC Officer.

(c) Any CIB/NCIC entry which cannot or has not been verified by the victim, insurance company, or official will immediately be canceled from the system. The entry may be re-entered at a later date if verification is received after cancellation.

(d) Verification of property (guns/parts/plats/vehicles/boats), is done by the Chief of Police and/or TAC Officer. Contact must be made with the original complainant or insurance company.

(e) Validations will only be done by the Chief of Police and/or TAC Officer. Other personnel may verify the persons or property are still wanted/missing/unidentified or stolen, but only validation officers may validate the records.

(f) It is the duty of Validation Officers to insure the accuracy of entries into the CIB and NCIC files. This also includes entry of all data available, whether entered immediately with the record or later entered as a modification or supplement.

(1) The Validation Officer is responsible to see that the validation is accomplished and the certifying letter returned to the CIB within the time period specified.
(2) The Validation Officer shall be appointed by the Chief of Police.

Sec. 6-5-11 Cancellations.

(a) **Cancellations.** TIME System entries should be canceled when one (1) of the following occurs:

(1) A locate ($L) message is received for the entry.
(2) An Emancipated Juvenile Warrant ($J) message is received for the entry. Check with the Chief of Police if the subject is to be re-entered as an adult after obtaining a new warrant.
(3) A Purged Record ($P) notice is received from NCIC. Any corresponding CIB record is then canceled by CIB, requiring no action by this Department. This record may be re-entered if the property is verifiable as stolen.
(4) The Department is notified that the property has been recovered. Do not wait until the property is in your possession, cancel immediately.
(5) The Department is notified the wanted/missing person has been apprehended or located, or a warrant has been otherwise satisfied. You are not allowed to wait until the person is in your custody, even if the arresting agency is holding the person pending outcome of their charges. The entry should be canceled subject to Section 6-5-9(a)(8).

(b) **Purged Records.** Purged records will normally not be re-entered unless there is some investigative value to re-entering the item to extend the retention period. Retention periods are as follows:

(1) ***Warrants.***
a. Warrants—indefinite.
b. Temporary Felony (Warrant)—forty-eight (48) hours.
c. Juvenile (Warrant)—indefinite.
(2) ***Missing.***
a. Juvenile—date of emancipation.
b. All other missing—indefinite.

(3) ***Unidentified Person.*** Nine (9) years plus year of entry.
(4) ***Vehicle.***
  a. By plate number—ninety (90) days.
  b. By vehicle identification number—four (4) years plus year of entry.
  c. Temporary felony—ninety (90) days.
  d. License plate—One (1) year after expiration year.
  e. Parts—four (4) years plus year of entry.
(5) ***Articles.*** One (1) year plus year of entry.
(6) ***Guns.***
  a. Stolen—indefinite.
  b. Recovered—two (2) years plus year of entry.
(7) ***Boats.***
  a. By registration—ninety (90) days.
  b. By hull number—four (4) years plus year of entry.
(8) ***Securities.*** Travelers checks/money orders—two (2) years plus year of entry.

(c) **Canceled Records.**

(1) Once a record has been canceled, the printout of the TIME System cancellation will be placed in the case jacket. The record should then be queried to ensure that it has indeed been canceled from the system.
(2) The cancellation should be noted on the TIME worksheet including the date and the operator canceling the record.
(3) If there is no information in the case explaining the reason for the cancellation (HIT confirmation/notice from court, etc.), a brief report should be included in the case with the reason for cancellation of entry.

Sec. 6-5-12 HIT Confirmation.

PROCEDURES:

(a) **HIT Confirmation Requests.**

(1) If a "HIT" is received on a TIME System query, the five (5) steps of HIT Confirmation will be followed. They include:
  a. Check the computer HIT against the original query.
  b. Check with the officer at the scene for additional information to clarify the HIT.
  c. Check with the "ORI" (entering agency) to verify the entry. [ten (10) minute rule].

d. Obtain hard copy from the ORI on the validity/disposition of the case/HIT.
e. Query all identifiable data not queried originally. (Social Security #, Owner Applied #, etc.).

(2) The ten (10) Minute Rule does not mean the ORI must confirm within ten (10) minutes, it means they have to acknowledge your message and let you know approximately how much time it will take to confirm the HIT.

(3) HIT Confirmation can only be done using the "HIT Confirmation" format on the Acer 910. HIT Confirmation may not be done by Administrative Message.

(b) **HIT Confirmation Responses.**

(1) When a request for HIT Confirmation is received, it is required that you respond within ten (10) minutes. This response must not necessarily contain the actual HIT Confirmation, but at least contain acknowledgement of the HIT request and approximate amount of time it will take to confirm the HIT.

(2) The officer receiving the HIT should retrieve the case involved and check the case to insure the entry is valid. If the entry is a felony, make sure that the requesting agency is within the extradition area specified. The operator should then advise the requesting agency of the validity of the HIT, and request information of that agency as to what they will be doing with the person/property.

(3) Once the HIT has been confirmed and the requesting agency advises they have the person/property in custody, the original entry should be canceled. If the HIT involves a person and the requesting agency will also be holding the person on their charges, the entry will still be canceled and an administrative message sent to the holding facility advising that this department requests the person be held for pickup on our local charges. If bond is posted and there is not a body attachment, this department must provide the defendant with a court date. Officers shall follow Section 6-5-9(a)(8).

Sec. 6-5-13 HIT Scoring.

POLICY:

TIME System agencies are required to report the number of CIB/NCIC HITS for each month to the TIME System Control Center (TSCC). The telecommunicator assigned to records will be responsible for reporting to TSCC all of the HITS scored and maintaining a HIT log. All original HIT confirmations and dispositions shall be placed in the "HIT Folder" file pending a monthly report being filed with the TIME System.

Sec. 6-5-14 NCIC Security.

PROCEDURES:

(a) **Personnel.**

(1) State and national record checks by fingerprint identification will be conducted on all employees prior to access being given to NCIC files. A CIB and FBI (blue) applicant fingerprint card will be submitted to the Crime Information Bureau. The purpose code J-NCIC Security Policy will be used in the "Applicant For" and Reason Fingerprinted" block of the fingerprint cards.

(2) If a criminal record or a wanted person record is found, NCIC access will be denied until the matter is reviewed. The Chief or designee will review and make determination. If determination is made that NCIC access would not be in public interest, such access will be denied.

(b) **Location Security.** Terminal access will be located within the Police Department and access will be restricted to the minimum number of authorized employees needed to complete the work. All visitors to the Police Department must be accompanied by staff personnel at all times; no unauthorized personnel shall be left near the terminal.

(c) **Violations.**

(1) No NCIC information is to be given to any unauthorized person.
(2) All requests for NCIC information (III) must be logged in NCIC Security Log.
(3) No NCIC information should be given out over the radio or telephone unless absolutely necessary.
(4) No III, NCIC, or CIB reports should be left in public view. If they are not attached to or included with a citation or incident report, they must be shredded.
(5) Copies of III, NCIC, or CIB reports should not be given out with photocopies of reports without authorization.
(6) Operators should use terminal access only for those purposes for which they are authorized.

(d) **Entry to NCIC/CIB Security Log.**

(1) ***Name.*** Enter the subject's name and date of birth you are running the query on.
(2) ***Date.*** Enter the date the query is being requested.
(3) ***Code.*** Enter the proper code used for the query from the list below:

C Criminal justice purposes.

E Authorized employment and/or licensing purposes. (Applicant checks for Police Officers and all criminal justice employee applicants *must* be submitted using Purpose Code J.)

J Criminal justice employment purposes. (Background or pre-employment checks.)

(4) ***For.*** Enter the person's name who requested the query.

(e) **$. Messages.**

(1) ***$.K—Missing Field.*** Means one (1) or more of the fields needed for the Missing Person file entry to remain in the system is missing.

This message should serve as a reminder to make contact with the source of a Missing or Unidentified entry to determine what additional information can be added to the entry. If the entry is modified or supplemented in any way, the entry will again be searched against other missing or unidentified entries.

(2) ***$.L—Locate Notification Message.*** Locate Notification Message is to indicate (until the originating agency cancels a record) that the record entry has been located or recovered. NCIC records are appended with Locate or No-Action Locate codes.

TIME System entries should be canceled when a locate message is received for the entry.

If the Locate is on a Missing Person entry NCIC policy results in an immediate cancel of the missing person. It is the responsibility of the ORI to immediately cancel this missing person record as it is not automatically canceled from the Crime Information Bureau Files.

(3) ***$.L—Agency Responsibility When a Locate ($L) Message is Received.*** Upon receipt of a locate notification, by either canceling the record (in the case of an action locate) or modifying the remarks to indicate your agency will not pick up in that state (in the case of a no-action locate). In the case of an action locate, NCIC will automatically cancel the NCIC record after ten (10) days if the record is not canceled by the "ORI". The second no-action locate placed on the record will automatically cancel the NCIC record. Remember that according to NCIC policy whenever a locate is received on a wanted person entry where extradition will occur, the record must be

removed from the NCIC File even though the wanted person has not been returned to your agency and is still awaiting extradition.

(4) ***$.J—Emancipated Juvenile Warrant Message.*** Check with the Chief of Police if the subject is to be re-entered as an adult after obtaining a new warrant.

(5) ***$.P—Purged Record Notice.*** Any corresponding CIB record is then canceled by CIB, requiring no action by our Department. This record may be re-entered if the property is verifiable as stolen.

(6) ***$.E—Serious Error.*** Serious error is determined either by the FBI, NCIC or CIB requires immediate attention by the entering agency. Therefore, a serious error notice is usually received by administrative message via the terminal that entered the record. FBI, NCIC will advise the Control Terminal Agency for Wisconsin (CIB) and the originating agency via terminal of an apparent serious error and request that it be verified, changed or canceled within twenty-four (24) hours. If neither a response is received advising the entry is correct nor corrective action is taken during that time period, CIB/NCIC will cancel the record.

Sec. 6-5-15 eTIME Policies; Security; Information Dissemination.

POLICY:

(a) **Appropriate Use of Information.**

(1) ***Dissemination Considerations.*** Data stored in databases of participating data service agencies are documented criminal justice system records, or administrative records containing sensitive personal information. These records must be protected to ensure correct, legal, and efficient dissemination and use.

(2) ***Misuse of System by Participating Agencies.***

a. Data service agencies have agreed to make information available to law enforcement and criminal justice professionals through the eTIME System for the specific purpose of facilitating the administration of criminal justice. Any misuse of this information or violation of these policies jeopardizes the availability of information for all participating agencies.

b. Any alleged misuse of the eTIME System will be investigated by the Crime Information Bureau (CIB). In the event of discovery of misuse, the Department will take corrective administrative action. Under state and federal law, individuals and agencies may be subject to criminal penalties if certain records are misused. Authorized users should also note that misuse of information obtained through the eTIME System could result in civil liability for both the user as well as the City of Stanley Police Department.

(b) **Secondary Dissemination of Information.**

(1) ***Proper Authorization Required for Information Dissemination.***

a. Any individual authorized to use the eTIME System who receives a request from any other individual for eTIME System information must ensure that the person requesting the information is authorized to receive the data before disseminating data to another person.

b. Each data service has its own rules for secondary dissemination of records. Some records are public, but can only be obtained by a direct public access request to the originating agency; a fee may be involved. Other records, especially federal criminal history records and state juvenile records, are confidential.

c. Most records may be legitimately disseminated to another criminal justice employee or agency where the purpose of the request is criminal justice related.

d. Secondary dissemination of federal criminal history records (III) must be logged.

(2) ***Proper Disposal Required.*** All eTIME System records must be properly disposed of by shredding paper or electronically deleting the record when it is no longer necessary to keep the record.

(3) ***Dissemination Records to be Kept with Paper Copies.*** Any criminal history record that is printed onto paper must have an accompanying entry in the secondary dissemination log maintained by the Chief of Police.

(4) ***Federal Criminal Records Checks.*** At present, eTIME does not permit federal criminal history checks to be conducted. All criminal history records obtained through eTIME will only be compliled through the State of Wisconsin, and, thus, shall not be deemed official criminal history records for the purpose of criminal prosecution. Criminal history checks that are required for official purposes shall be obtained through the Communications Center.

(5) ***Dissemination Limited to Sworn Department Members.*** No criminal history record compiled through eTIME shall be disseminated outside of sworn officers employed by this Department and shall be destroyed immediately upon the record fulfilling its usefullness in an investigation. For tracking and auditing purposes, all criminal history checks shall include the identity of the requesting user in the "attention line". This identity may be the user's badge number, name, or any other information that specifically identifies the user.

(6) ***Electronic Copying or Retransmittal Prohibited.***

a. No user shall, at any time, electronically copy, and/or electroncially retransmit information obtained through the eTIME System through any other electronic communications resource. This shall include, but not be limited to, facsimile and electronic mail.

b. All electronic transmission of information obtained through eTIME transactions shall be encrypted and this requirement is not typically available through other

means of electronic communication without additional hardware or software support, which is not provided by this Department.

(c) **Authorized Use.**

(1) ***Use Authorization Required.*** No individual may use the eTIME System without the authorization of the Chief of Police (and TIME Coordinator, if the Department utilizes such a designee). The Department is responsible for eTIME System use by all such individuals it authorizes, including its support, maintenance, contract, and vendor personnel who maintain server and network equipment carrying eTIME System messages.

(2) ***Required Background Checks of eTIME Users.***

a. No individual shall be authorized to use, support, or maintain the eTIME System unless he/she has been subject to a fingerprint-supported criminal background check. The Department shall conduct background checks of all operational employees and support, contract and vendor personnel who maintain server and network equipment carrying eTIME System messages who have:

1. Access to terminal equipment capable of initiating eTIME System transactions;
2. System-level log-on privileges to servers and network equipment carrying eTIME System messages; and
3. Generalized log-on privileges to the eTIME System from any computer equipment.

b. No person with a prior conviction for a felony offense is authorized to use, support, or maintain the eTIME System. Other offenses may be disqualifying at the discretion of the Chief of Police or the Director of the Crime Information Bureau.

(3) ***Disclosure of Access and Password Information Prohibited.*** Authorized users of the eTIME System shall not disclose their access information, including user ID and passwords, to any other individual, whether he/she is authorized or not to use the eTIME System. Authorized users of eTIME shall only connect to eTIME using only his/her assigned User ID and password combination.

PROCEDURES:

(a) **Training.**

(1) ***Basic Training Requirements.*** Any individual using the eTIME System under its authority will be trained in the operation of equipment and system policies/procedures. Initial training shall occur within six (6) months of employment or assignment to a

position with eTIME System access privileges. This training will include a test to affirm the operator's proficiency and knowledge of data services connected to the eTIME System.

(2) ***Biennial Testing.*** All authorized users will be re-tested biennially to reaffirm operating proficiency. The level of training will be based on system use. At present, the first three (3) online training modules are required to utilize the eTIME System; however, users are encouraged to complete at least the first six (6) online training modules to make biennial re-testing quicker and easier for the user.

(b) **Software Updates.** Occasionally, the Crime Information Bureau will implement updates to the eTIME System. Some of these updates will include new transactions that can be processed by authorized users. No authorized user shall use, or attempt to use, any new transaction implemented by the Crime Information Bureau without first being trained on appropriate use of the new transactions.

(c) **Security.**

(1) ***User Responsibility for Securing Information.*** Each authorized user of the eTIME System ultimately has the responsibility of securing the information he/she exchanges on the eTIME System. This includes, but is not limited to, ensuring that all printed copies of records obtained through the eTIME System are not available for viewing by members of the general public and not processing eTIME transactions in the presence of any member of the general public.

(2) ***Leaving Open Terminal Connection Unattended Prohibited.*** No authorized user of eTIME shall leave an eTIME terminal connection open while he/she is not in the general presence of the terminal so other individuals may gain access to the information contained in the eTIME System.

(3) ***Regulations Regarding Security with Federal Crime Information.*** Federal regulations provide for strict adherence to stringent security codes relating to information obtained through the NCIC data source agency. To ensure such security codes are safeguarded and to ensure the integrity of the eTIME System, access to the eTIME System shall be restricted to computer terminals approved by the Chief of Police and/or the Department's TIME Agency Coordinator (if position established). This restricts access to the eTIME System from any personal computer at any user's home or other work place.

(4) ***Reporting Security Compromises.*** All security compromises shall be forwarded to the Crime Information Bureau for investigation and subsequent sanctions by the Crime Information Bureau as deemed appropriate.

(d) **Passwords.** All authorized users shall follow the below listed guidelines for generating his/her password for the eTIME System. The eTIME software strictly and automatically enforces these guidelines:

(1) Passwords *shall* be between eight (8) and twenty (20) characters in length.
(2) Passwords *shall* contain at least one (1) numeric digit.
(3) Passwords *shall* contain at least three (3) of the four (4) categories: upper case letters, lower case letters, digits from 0 to 9, symbols found on the keyboard (~!@#$%^&-*()_+, etc.).
(4) Passwords *cannot* be any of the previous ten (10) passwords used on the account.
(5) Passwords *cannot* contain any portion of the User ID.
(6) Passwords *cannot* match the User ID.

(e) **TIME Agency Coordinator (TAC).** This Department shall name a person as the TIME System Agency Coordinator (TAC); the person so designated may be the Chief of Police. The TAC shall be the primary contact person with the Crime Information Bureau for operational, technical, and security matters. The TAC is responsible for ensuring all authorized users are appropriately trained and is documenting the training progress for all authorized users. Additional responsibilities the TIME Agency Coordinator shall carry out are outlined in the document "TIME Agency Coordinator Responsiblities" as published and updated by the Crime Information Bureau.

(f) **Wanted/Stolen Vehicle Hits.**

(1) ***Required Actions.*** Any authorized eTIME user that queries a vehicle identification number (VIN) or license plate number and obtains a stolen vehicle entry based on that query shall perform both of the following two (2) actions within fifteen (15) minutes of receiving the stolen vehicle entry:
   a. Notify the Communications Center of the query and the result and any circumstances surrounding the query. All messages from other agencies to this Department via the TIME System are to be forwarded to the Communications Center.
   b. Through email, the Officer shall notify the TIME Agency Coordinator and Chief of Police of the query and the result and any circumstances surrounding the query. Questions may be sent to this Department regarding the query and the circumstances involved and will be directed to the TIME Agency Coordinator and/or Chief of Police.

(2) ***Timing of Inquiries.*** Circumstances surrounding TIME inquiries include the reason for the query. Occasionally, during routine patrol, an Officer may observe a vehicle that appears questionable but opts not to have the Communications Center query the vehicle in question, perhaps because the Officer is involved with a high risk situation occurring in another jurisdiction. The Officer may return to the office and query the vehicle through eTIME and produce a stolen vehicle entry on the vehicle. It is important for the Officer to accurately recall where the vehicle was located, which

direction the vehicle was headed, how many occupants and the description of the occupants, including the identity of any known occupants to assist in the investigation efforts of the requesting agency.

(3) ***Notification to the Communications Center.*** Notification to the Communications Center is required with all queries of vehicles resulting in a stolen vehicle hit. Agencies entering stolen vehicle information tracking dates and times that other law enforcement agencies query the vehicle information to follow up on the investigation of the stolen vehicle later. Many times stolen vehicles are recovered later after a period of time, and typically they are recovered without the operator of the vehicle being known. In this case, the entering agency will contact all other agencies that queried the vehicle to determine where the vehicle was/is and obtain possible suspects or persons of interest in the investigation. This contact shall be sent to the Communications Center on behalf of the City of Stanley Police Department and may come minutes, hours or even days after the Officer make the inquiry regarding the vehicle.

(g) **Disciplinary Measures.** Disciplinary measures for violations of the policies/procedures of this Chapter and all other rules, regulations and laws governing the use of the eTIME System are to be consistent with the disciplinary policies governing the City of Stanley Police Department.

Title 6 ▸ Chapter 6

Computer and Internet Use; Cellular Telephone Use

Sec. 6-6-1 General Computer, Telecommunications, Email and Voice Mail Use Policies.

POLICY:

(a) **Rights of the Department as Conditions of Employment.** The City of Stanley Police Department's computer, email, telephone, fax, internet, data storage and voice mail equipment and systems are business tools intended for official purposes and Department administrative functions, and to facilitate official communications. These systems belong to the Department and any and all information, communications or other material transmitted or stored on any Department computer, email, internet, pager, telephone, fax, data storage and voice mail equipment and systems are subject to inspection. The Department retains the right to access, examine and/or disclose any material transmitted or stored on its equipment or systems at any time without regard to content.

(b) **Right of Ownership; Inspections; Privacy.**

(1) ***Department Ownership; Privacy Limitations.*** Although employees may have passwords to access such equipment and systems, employees shall not construe passwords as creating any expectation of privacy. Employees should not assume that any documents or data that they store on or process through the Department's computer, email, internet, pager, telephone, fax, data storage and/or voice mail equipment or system or any email or voice mail messages that they receive or send

are confidential. These systems are provided to assist employees in the performance of their jobs and responsibilities pertaining to Department business.

(2) ***Inspections and Monitoring.*** The Department may monitor, inspect, search, transfer, access/disclose, scan or copy data, correspondence, documents, files or other information, both stored or in real time, on any and all technology resources owned by the Department. The Department is the owner of all data/information stored on email, voice mail, servers, centralized storage, and Department-provided computers/telecommunications equipment. All emails on the Department computer system are presumed to be public records, unless falling within a recognized non-disclosure exception of the Wisconsin Open Records Law, and contain no right of privacy. The data/information remains subject to all state and federal copyright laws. Personal information shall not be stored on Department-owned computers/equipment and is subject to inspection. The Department has the right to monitor, limit, or restrict access to its technology resources, including, but not limited to, the following:

a. Investigating employee misconduct, including sexual harassment and racial discrimination;
b. Responding to requests pursuant to the Wisconsin Open Records Law; and
c. Protecting against illegal activities by employees, for which the Department, as an employer, may have liability exposure.

(c) **Copyright Compliance.** Employees must comply with all copyright and intellectual property laws with respect to the use of the Department's technological and electronic resources.

(d) **Disciplinary Actions Upon Noncompliance.** Failure to comply with the policies in this Chapter may result in discipline under this Personnel Manual, including termination.

(e) **Rules Regarding Use of Department Computer and Telecommunications Equipment.**

(1) ***Improper Use of Coopyrighted Material on Department Equipment.*** The Department computer system shall not be used to download, copy, or store any copyrighted software, publications, music, video, or other content without permission from the copyright holder and appropriate Department supervisor.

(2) ***Illegal or Improper Department Computer Use.*** The Department computer system shall not be used for any activity, or to transmit any material, that violates United States, State of Wisconsin or local laws. This includes, but is not limited to, fraudulent acts, violations of copyright laws, and any threat or act of intimidation or harassment against another person. Use of the Department computer system for hate mail, defamatory statements, vulgar, derogatory, or obscene language statements intended to injure or humiliate others by disclosure of personal information (whether

true or false), personal attacks on others, and statements expressing animus towards any person or group by reason of race, color, religion, national origin, gender, sexual orientation or disability if not acceptable.

(3) ***Improper Anonymous Postings.*** Department computer system users shall not post anonymous messages or attempt to impersonate another person by forging email, web pages or other electronic media.

(4) ***Unauthorized Accessing of Others' Accounts.*** Without express permission, Department employees may not log on to another user's account, IP address, or other network codes, attempt to access another user's files, or permit anyone else to log on to log onto their own accounts if they are unauthorized to do so. Users may not try to gain unauthorized access ("hacking") to the files or computer systems of any other person or organization.

(5) ***Prohibited Sites.*** Unless part of an official law enforcement investigation, users of Department computers shall not access websites, newsgroups, or chat areas that contain material that is pornographic or prohibited child pornography laws, or that promotes illegal acts.

(6) ***Personal Use.*** The primary use of the Department computer system and internet is for Department-related work. While some incidental personal use of Department equipment is permitted, such incidental use will not be deemed a waiver of the Department's right to prohibit all such use, either on an individually-applicable or on a generally-applicable basis, nor will such private use be implied as creating a privacy right contrary to the policies of this Chapter. Such occasional personal use shall not detract from employees' primary work responsibilities with the Department.

(7) ***Spamming.*** Department computer system users shall not engage in "spamming" (sending unofficial electronic communication to large groups of people) or participate in private chain letters.

(8) ***Damage to Department-Owned Equipment.*** Department computer system users who maliciously access, alter, delete, damage or destroy any computer system, computer network, computer program, or data may be subject to disciplinary action by the Department, and possible criminal prosecution. This includes, but is not limited to, changing or deleting another user's account; the unauthorized changing of the password of another user; using an unauthorized account; deliberately damaging or deleting Department records and files; destroying, modifying, vanalizing, defacing or abusing hardware, software or other electronic media equipment of the Department.

Sec. 6-6-2 Computer Hardware Rules.

POLICY:

(a) **Internet Use.** Internet use shall be governed by the policies in Section 6-6-5 of this Manual. Unauthorized internet use is prohibited.

(b) **Unauthorized Modifications.** Once a computer system is set up and running to work efficiently with the Department-owned software, employees shall not adjust or change any hardware switches, settings, or make any other major modifications or changes to the computer system without prior approval from a supervisor, or whomever is designated as being responsible for the computer system.

(c) **Protection of Equipment.**

(1) Electric charges and static electricity can destroy computer equipment, software and data. Users should never plug or unplug the computer or any peripheral equipment from the A.C. wall power outlet while any piece of said computer equipment is switched to the "on" position.
(2) Users should never plug or unplug any cable connecting the computer or any peripheral while any part of the system is switched on.
(3) During seasons of the year when static electricity is more prevalent, users should always touch a metal object such as a desk (away from and not the computer desk) or other metal object to dissipate static charges before using the computer.
(4) Users should never set any container of liquid of any kind on top of or next to the computer. One (1) drop of any kind of liquid can destroy an expensive system very quickly.
(5) Users should not stack books, manuals or other items against the computer when it is operating. Electric equipment produces heat, which is an enemy to safe operation of computer equipment. The computer is cooled by an internal fan, and when vents on the computer are blocked, heat will build up.
(6) Users should not move or jar the computer or computer desk while the computer is in operation as the hard drive is a continuously spinning device. Any movement could cause a "head crash" resulting in permanent damage to the hard drive and loss of data.

Sec. 6-6-3 Software Policies.

POLICY:

(a) **Use of Department-Supplied Software.**

(1) Certain software items (computer programs) are supplied by the Department for use for Department-related work. Users shall not change any settings or setup sections of any Department software without prior approval from the Chief of Police or his/her supervisor. Any software that is installed must be properly licensed from the

copyright owner thereof, and any modifications must comply with the terms of the applicable license(s).

(2) Users shall not make copies of any software for any person, as unauthorized copying of copyright material such as computer software is illegal.

(3) Users shall not loan out any Department software or any printed material (manuals, instruction books, reference books) accompanying Department software.

(4) Users shall not erase, delete, or change any Department software in any way.

(5) Do not use Department software for any personal business or use without prior approval from the Chief of Police.

(b) **Non-Department Supplied Software.**

(1) Other software not owned or acquired by the Department may be used or may be required to perform tasks or business for the Department; however, any non-Department software must be used only for Department business and then only after approval from the Chief of Police and the Department official responsible for the Department's computer systems. Forbidden programs include, but are not limited to, unlicensed software, pirated music, and pornography.

(2) Due to the abundance of "virus" or "trojan" programs that have surfaced which maliciously invade a computer system and destroy data or even equipment, only software from a secure or known source shall be submitted for approval by a supervisor. Secure or known sources include: all legal commercial software, shareware or public domain software. In the case of shareware or public domain software, it will be considered to be from a secure or known source if the software comes directly from a commercial distributor or directly from the author of the software. Insecure or unknown sources include software obtained through friends or acquaintances where the history or path of the software is unknown, and any software that has been acquired from a computer bulletin board type service.

Sec. 6-6-4 General Computer User Rules.

POLICY:

(a) **Municipal Use Purpose.** With limited exceptions described in this Chapter, Department computers are for municipal business only and any other unspecified use requires express approval from the Chief of Police.

(b) **Permitted File Copying.** When an employee uses the computer to prepare a report or record any other municipal business, that employee may save a copy of said report onto a

flash drive, DVD, CD, or other storage medium with an appropriate file name for future reference.

(c) **Security Considerations.** Reports, data files and other information stored in the computer or on the individual employee's DVDs, CDs, flash drives, external hard drives, etc. may contain sensitive information and should be maintained with the same security as any other sensitive or legally confidential information.

(d) **Intradepartment Access.** Only employees designated by the Chief of Police shall have general access to all of a department's computer and related equipment.

(e) **Recreational Use Prohibited.** Department computers are for municipal business only and should not be used for playing computer games or simulations or for other leisure activities.

Sec. 6-6-5 Internet and Social Media Use.

POLICY:

(a) **Authorization.** Internet, social media, and email use on Department equipment is authorized by the Chief of Police consistent with the policies of this Chapter.

(b) **Purpose.** This policy is intended to both identify the circumstances under which the Department's employees may access the internet through Department equipment/facilities, or when identified as Department employees, and define what the Department considers acceptable use and conduct on the internet and similar telecommunications devices. This policy's purpose is to clearly communicate expectations with respect to what is and what is not "acceptable use" and to minimize the risk of offensive or inappropriate behavior on the internet.

(c) **City Property.** All Department computer systems that access the internet are the property of the City of Stanley Police Department. These systems are subject to monitoring, inspection or servicing at any time without notice. Internet access granted to employees shall comply with all of the requirements set forth herein. This policy applies to all Department/municipal computer systems or whenever the user identifies himself/herself as a Department employee or agent.

(d) **Potential Social Media Site Use by the Department.**

(1) Social media can be a valuable investigative tool when seeking evidence or information about:

a. Missing persons;
b. Wanted persons;
c. Gang participation;
d. Crimes perpetrated online (i.e., cyberbullying, cyberstalking, etc.); and
e. Photographs or videos of a crime posted by a participant or observer.

(2) Social media can be used for community outreach by:
a. Providing crime prevention tips;
b. Offering online reporting opportunities;
c. Sharing crime information and data; and
d. Soliciting tips about unsolved crimes (i.e., Crimestoppers, text-a-tip).

(3) Social media can be used to make time-sensitive notifications related to:
a. Road closures;
b. Special events;
c. Weather emergencies; and
d. Missing or endangered persons.

(4) For persons seeking employment and volunteer positions with the Department, social media can be a valuable recruitment tool.

(e) **General Internet Use Procedures.**

(1) ***Purpose; Acceptable Use Compliance.*** Internet services are provided by the Department to support open communications, the exchange of information and the opportunity for collaborative government-related work. The Department authorizes the use of electronic communications by employees. Although access to information and information technology is essential to the missions of government agencies and their users, use of internet services is a revocable privilege. Conformance with acceptable use, as expressed in this policy, is required.

(2) ***Employee Compliance as a Condition of Employment.*** Employees are required as a condition of employment to become familiar with this policy and what constitutes acceptable and unacceptable internet use, before accessing the internet on any Department computer system. Employees are also required to remain current on this policy, and other work rules, notices, memos, and other communications related to the use of the internet. The responsibility to remain current and in compliance with internet use restrictions lies with each employee. Compliance with applicable acceptable use restrictions is mandatory.

(3) ***Adherance to Professional Standards of Communications.*** Employees are bound by Department regulations, work rules and policies related to professional standards of communications while using the internet. Employees shall avoid uses of the network that reflect poorly on Department government. Employees should also know and follow the generally accepted etiquette of the internet. For example:

a. Use civil, professional forms of communication;
b. Respect the privacy of others;
c. Respect the legal rights provided by copyright and licenses to programs and data;
d. Respect the privileges of other users;
e. Respect the integrity of computing systems connected to the internet.
f. Avoid the use of slang terms or overly informal forms of communication.

(4) ***Applicability of Ethical Standards.*** Users should remember that existing and evolving rules, regulations, and guidelines on ethical behavior of government employees and the appropriate use of government resources apply to the use of electronic communications systems supplied by the Department.

(f) **Approved Internet Uses.** Specifically authorized internet uses include, but are not limited to, the following:

(1) ***Department Communications.*** Communications and information exchanges directly related to the mission or work tasks of the Department.
(2) ***Professional Development.*** Communications and exchanges for professional development, to stay current with training or education, or to discuss issues related to Department activities and work.
(3) ***Grants and Contracts Administration.*** Use in applying for or administering grants or contracts for Department programs.
(4) ***Research.*** Use for researching standards, analysis, and professional society activities related to the employee's work tasks and duties.
(5) ***Communications Regarding Regulations.*** Announcements regarding, or research into, new laws, procedures, policies, rules, services, programs, information, or activities.
(6) ***Non-Security Sensitive Communications.*** Any other governmental administrative communications not requiring a high level of security.
(7) ***Incidental Acceptable Communications.*** Communications incidental to otherwise acceptable use, except for illegal or specifically unacceptable uses.
(8) ***Investigations.*** Use for authorized official investigative purposes.
(9) ***Limited Personal Use.*** Personal use is permitted provided that it should not unduly interfere with official duties.

(g) **Prohibited Internet Uses.** Prohibited internet uses include, but are not limited to, the following:

(1) ***Illegal Purposes.*** Use of the internet for any purposes that violate a Federal, State or Department statute, ordinance or personnel policy, unless the use is for authorized investigative purposes.

(2) ***Accessing Inappropriate Sites.*** Use for access to and distribution of (except as authorized for investigative purposes):
   a. Indecent, obscene, sexually explicit or offensive material;
   b. Pornography; or
   c. On-line games.

(3) ***Computer Games.*** Use to access distribution of computer games that have no bearing on the Department's mission. Simulations that help teach, illustrate, train, or simulate agency-related issues may be acceptable. Employees wishing to use such simulation programs should obtain permission from their supervisor before use.

(4) ***Activities Which Disrupt Department Computer System.*** Use of internet services so as to interfere with or disrupt Department computer network users, services, or equipment.

(5) ***Confidential Information.*** Intentionally seek out or distribute information, obtain copies of, or modify files and other data, which is private, confidential, or not open to public inspection or release unless specifically authorized.

(6) ***Impermissible Copying of Software.*** Intentional copying of any software, electronic file, program or data without a prior, good faith determination that such copying is, in fact, permissible. Any efforts to obtain permission should be adequately documented.

(7) ***Misrepresentation of Identity.*** Intentionally representing oneself as someone else, either on the Department's system or elsewhere on the internet, unless explicitly authorized to do so by those other users. Users shall not circumvent established policies defining eligibility for access to information or systems.

(8) ***Harassment.*** Intentionally developing programs designed to harass other users or infiltrate a computer or computing system and/or damage or alter the software components of the same.

(9) ***Unauthorized Solicitation.*** Use for unauthorized fund raising or public relations activities not specifically related to the City of Stanley.

(10) ***Discriminatory Transmissions.*** Transmission of discriminatory, defamatory or harassing email is prohibited. Infractions of this rule are a violation of the Department's harassment policy. All potentially harassing email wil be investigated, and violators will be disciplined under the Department's harassment policy.

(11) ***Copyrights.*** Transmission of email containing confidential, proprietary, or trade secret information is prohibited. Employees shall comply with all copyright and intellectual property laws with respect to the use of the Department's technological resources. Access to this information is to be carefully restricted.

(h) **Computer Viruses on Downloaded Software.** Any software/files downloaded should be virus checked prior to use. This should be done prior to introducing files from any outside source into the Department's system through a flash drive, CD, DVD or the internet.

(i) **Contractor Access.** Contractors and other non-Department employees may be granted access to Department-provided internet services at the discretion of the contracting authority. Temporary addresses must be under strict supervision with appropriate audit techniques implemented and reviewed. Temporary addresses must be deleted immediately upon non-Department employee and contractor's departure or the end of the project requiring access to the internet.

(j) **Password Use.**

(1) ***Usage Standards.*** Users shall only use passwords associated with the Department's information system. When setting up an account at a different information system that will be accessed using the internet, employees shall choose a password that is different from ones used on Department equipment. Users shall not use the same password for both local and remote internet-accessed systems. If the password used at the internet-accessed remote site were to be compromised, the different password used locally would still be secure. Passwords should not be so obvious so that others could easily guess them, and passwords should be periodically changed. All passwords must be disclosed upon a request by the Chief of Police or designee.

(2) ***Improper Use of Another User's Password.*** Employees are prohibited from using any other employee's passwords to gain access to fellow employees' files unless expressly authorized.

(k) **Logoff (Exiting).** Employees should always make reasonable attempts to complete the logoff or other termination procedure when finished using a remote, internet-accessed system or resource. This will help prevent potential breaches of security.

(l) **Email Security.**

(1) ***Types of Social Media.*** Unencrypted electronic mail sent or received on the internet cannot be expected to be secure. Email communications generally are not considered private and are often classified as public records. Communications made on a Department system are subject to monitoring without notice to ensure that the Department's system is being used properly. Emails and other communications are the property of the Department and are not private.

(2) ***Public Records Considerations.*** The rules for retaining or deleting emails are the same as they are for printed correspondence. Most government-related emails are considered to be public records. Any "junk" or unauthorized email should be deleted on a regular basis. Email that contains information subject to record retention rules must be kept as long as required by law. The provisions of Chapter 19, Wis. Stats., are applicable to email.

(m) **Social Media Use.**

(1) ***Types of Social Media.*** "Social media" outlets and technology include, but are not limited to given ever-emerging technological tools:

a. Social networking sites such as Facebook, LinkedIn, and MySpace.
b. Blogs.
c. Microblogs such as Twitter.
d. Video sharing sites such as YouTube, Instagram, and iReport.
e. Photography sharing sites such as TwitPic and Flickr.
f. Wikis (shared encyclopedias) such as Wikipedia.
g. RSS feeds.
h. Mobile telephone content uploaded to the internet.

(2) ***Liability Considerations.*** Department officials and employees should always keep in mind that any use of social media — whether as official voice of the Department, municipality, voice for elected officials or as personally used by Department staff/employees — has the potential of creating an embarrassing situation for the Department. In some instances, the potential exists that the Department could face legal challenges if false, incorrect or non-public information is posted on a site used officially by the Department or personally be an employee.

(3) ***Official Social Media Use by the Department.*** The Department may choose to have an official presence representing the Department and its departments/programs on a social media site(s). The following policies should guide such social media use:

a. The Department should designate specific employees/officials responsible for maintaining the Department's presence on social media sites. Official Department social media presence shall not commence without prior approval by the Common Council.
b. Social media account names on Department-sponsored sites shall clearly be linked to the Department so that it is apparent to visitors and "friends" that they are receiving information from the Department. For example, the City of Stanley Police Department could name its Facebook page "City of Stanley Police Department", its Twitter account "City of Stanley", etc. Department staff members responsible for officially representing the Department on social media sites shall indicate that they work for the Department; all staff who use social media sites shall include a Department-designated prefix on their account names, similar to those used with email. For example, the Chief of Police might be "City of Stanley Chief of Police John Doe" on Facebook and "CH-John Doe" on Twitter.
c. Profile information for pages maintained by designated Department employees should include the employee's Department job title, Department website address, Municipal Building street address, telephone/fax numbers, and other relevant information.

d. Employees using Department-designated social media outlets should always be mindful that personal or political opinions are inappropriate in an official Department social media communication unless the Department has specifically asked that employee to share personal views and comments. In such instances, the employee sharing his or her comments should clearly identify the comments made as the employee's own opinions, not those of the Department.

e. Where possible, social media pages should state that the opinions expressed by visitors to the page do not reflect the opinions of the Department. Pages shall state that posted comments will be monitored and that the Department reserves the right to remove obscenities, off-topic comments, and personal attacks. Pages shall indicate that any content posted or submitted is subject to public disclosure.

f. Employees using a Department-designated social media outlet should always be factual and respectful with such communications, always maintaining confidentiality and privacy where appropriate. Employees should always check to make sure that they are not inappropriately sharing non-public information; examples of such information that shall never be posted on a social media site are matters related to co-workers, closed sessions of a governmental body, legally confidential records, personnel data, medical information, lawsuits or claims, or other non-public or confidential information. If there are questions, the employee should consult with the Chief of Police or the City Attorney.

g. Official communications should always be fact-checked before being posted on any social media site. Potential errors could create issues for the municipality ranging from minor to significant, and could potentially create unforeseen liability issues.

h. Any factual mistake made on a Department-designated social media site shall be corrected as soon as possible. If an entry is being corrected, the employee should both modify the earlier post containing the error and make it clear that the posting has been corrected. A timely correction is important to minimize the liability concerns for the Department if an outside party had acted on incorrect information officially posted by the Department.

i. Postings on a Department-designated social media site shall not include any content that violates any Department policies, that exhibit discrimination, harassment, pornography. libelous or otherwise defamatory content. Do not post content that a reasonable person may not consider maintains the dignity and decorum appropriate for local government.

j. Postings on Department-designated social media sites shall not include material that would give the appearance of affiliating the Department with or advocates for a political party or candidate running for public office.

k. Employees shall not post any photograph or video without the permission of each person in the photograph or video; a limited exception may be large "crowd shot"

pictures taken at a public meeting (i.e. "there was good public attendance at the hearing on the new comprehensive plan"). Do not post the name of any individual without the permission of that person.

l. Caution should be exercised when referring site visitors to third-party sites to make sure the content of such site is appropriate.

m. Employees should always keep in mind that postings to Department-designated social media sites are likely public records under Wisconsin law.

n. Content of social media sites used for recruitment for Department employment are subject to the same anti-discrimination and records retention standards as any other form of advertising for employment positions. Department officials conducting background checks during the recruitment process shall not violate the terms of use of any social networking site, nor shall employment candidates be asked to disclose their passwords to personal sites.

o. Under the Stored Communications Act (18 U.S.C. Secs. 2701 to 2712), an employer who uses illicit or coercive means to get into, or view, a person's social media accounts, the employer may possibly put itself at risk of violating this broadly worded Act. However, case law interpreting the Act has found that municipal employees who are on notice that messages on a municipality's communications/computer systems are public information are not able to use the Act to absolutely shield their communications. The Act also prohibits a provider of communications services from divulging the content of correspondence sent and received through its servers to anyone except the sender and the addressee, without the lawful consent of the same parties. As a result, iPhones, BlackBerry devices or cell phones purchased by the muncipality for its employees might not be able to request from the service provider companies transcripts of their employees' communications using those devices.

p. Internet profiles may disclose considerably more personal information regarding the poster than a prospective employer is legally permitted to consider when making employment decisions (i.e. disability, age, race, religion, pregnancy, marital status, national origin, ethnicity, etc.).

(4) ***Personal Use of Social Media Sites By Department Employees.***

a. Personal social media account names should not be tied to the Department (for example, a photograph posting of a Department law enforcement officer with badge and uniform). Employees should avoid inappropriate use of Department time/resources when engaged in personal use of social media sites (e.g. for profit or political activity).

b. Individuals who use personal social media accounts are not immune from the law, or from the need to follow Department policies and guidelines related to social media use, harassment prevention, media relations, computer use and other adopted Department policies. Be mindful that the lines between public and

private, personal and professional are blurred in online social networks. As a general guideline, employees should ensure that personal account content associated with the employee is consistent with the employee's work with the Department. Supervisors should exercise caution that off-duty postings, texts, cell phone messages, etc. to subordinates must still be professional and not suggest any harassment, discrimination or retaliation.

c. If a person is new to employment with the Department, be sure to review and update your social profiles to reflect the Department's policies.

d. As a general guideline, remember that "if it is on the internet, it is likely never truly private". Some social media sites, like Facebook, allow profiles to be limited by networks (i.e. schools) or friends of friends, both settings that make it easy for complete strangers, perhaps strangers who do not have the best interests of the person at heart, to examine the content. For example, profiles on Facebook may be set as private, but when photographs are added they have to be added with settings stating that only "friends" can view the photographs, or else parties who are not designate "friends" can view the photographs. Department members must always be mindful that privacy settings and social media sites are constantly in flux, and they should never assume that personal information posted on such sites is protected. Unlike oral communications, social media conversations remain somewhere and does not truly go away: the site cache, a hard drive, on a telephone's memory, etc. This guideline is equally applicable to text messages, voice mails, etc.

e. Department employees do not have the right to post Department non-public and confidential information through their personal accounts, such as information related to co-workers, personnel data, medical information, claims or lawsuits against the Department, etc.

f. Employees shall not use Department-owned equipment to post to personal sites content that violates Department policies.

(n) **Large File Transfers and Internet Capacity.** The internet connection is a shared resource. While routine electronic mail and file transfer activities will have a minimal impact on other users, large file transfers and intensive multimedia activities will impact the service levels of other users. Users contemplating file transfers over ten (10) megabytes per transfer or interactive video activities should be considerate of other users; schedule these activities early or late in the day or, better, after business hours.

(o) **Inappropriate Electronic Discussions.** Users should avoid being drawn into discussions where disclaimers such as "this represents my personal opinion and not that of the City or my Department" need to be used.

(p) **Responsibilities.**

(1) ***Superisor's Responsibilities; Violations.*** Supervisors are responsible for their employees' compliance with the provisions of this policy and for investigating non-

compliance. Suspension of service to users may occur when deemed necessary to maintain the operation and integrity of the Department's network. User accounts and password access may be withdrawn without notice if a user violates the acceptable use policy and other policies in this Chapter. Discipline may be imposed in cases of non-compliance with this policy. Criminal and/or civil action against users may be appropriate where laws are violated.

(2) ***Changes in User Status.*** Within two (2) business days of an employee's death, disability, or termination, the employee's supervisor shall notify the Chief of Police of the need to terminate access or change the user information.

DEFINITIONS:

The following definitions shall be applicable in this Chapter:

(a) **Blog.** A self-published commentary or diary on a particular topic that may allow visitors to post responses, reactions, or comments.

(b) **Page.** The specific portion of a social media website where content is displayed and managed by an individual(s) with administrator rights.

(c) **Post.** Content an individual shares on a social media site or the act of publishing content on a site.

(d) **Profile.** Information that a user provides about himself/herself on a social networking site.

(e) **Social Media.** A category of internet-based resources that integrate user-generated content and user participation. This includes, but is not limited to, social networking sites (Facebook, MySpace, LinkedIn), microblogging sites (Twitter, Nixle), photo- and video-sharing sites (YouTube, Flickr, Instagram), wikis (Wikipedia), blogs, and news sites (Digg, Reddit).

(f) **Social Networks.** Online platforms where users can create profiles, share information, and socialize with others using a range of technologies.

(g) **Speech.** Expression or communication of thoughts or opinions in spoken words, in writing, by expressive conduct, symbolism, photographs, videotape, or related forms of communication.

(h) **Wiki.** Web pages that can be edited collaboratively.

Sec. 6-6-6 Mobile Communication Device (Cellular Telephone) Use While On Duty.

POLICY:

(a) **Purposes.**

(1) Cellular telephones and similar devices have become essential in daily operations. Cellular telephones can be of great value and use by personnel in their everyday duties. The purpose of this policy is to set forth guidelines for the proper use of cellular telephones, pagers and other similar mobile communication devices (MCDs). This policy does not address the use of mobile data terminals (MDIs).

(2) It is the policy of the City of Stanley Police Depatment to use MCDs in the course of law enforcement operations to enhance departmental communications. MCDs may be used by Officers to conduct official business when the use of radio communication or landline telephones is unavailable, inappropriate, or inadequate to meet communication needs, provided the device is used in accordance with Department policies. Department members shall not use MCDs in any manner which would constitute disruptive activity.

(3) Data, information, photographs, videos, etc. stored in Department-issued or personal MCDs related to the course and scope of employment are the property of the Department.

(b) **Mobile Communication Device Use While On Duty.** The Department reserves the right to deny the use of any personal MCDs while the Department member is on duty. When so authorized, Officers electing to carry personally-owned MCDs while on duty shall provide the Chief of Police with the MCD's calling number.

(c) **Employees Having Personally-Owned Cellular Telephones, Personal Pagers or MCDs in Their Possession While on Duty.**

(1) The carrying of a personal cellular telephone/MCD is permitted while on work duty, subject to the procedures outlined in this Section. Employees may carry their personal cellular telephones while on work duty. The Department accepts no responsibility for loss or damage to personal MCDs. The carrying/use of a personal cellular telephone or MCD should not interfere with an employee's official duties.

(2) Use of personal cellphones or MCDs either in voice or data transmission while on duty should be restricted to essential communications and should be limited in length. Engagement in multiple or extended conversations unrelated to Department business or similar use that interferes with the performance of a duty is prohibited. Personal MCDs are subject to the use and safety policies of this Section.

(d) **All Department Cellular Telephone/MCD Use Should Be Limited To Appropriate Uses Only.**

(1) Department personnel with Department radios shall answer radio communications before answering their MCDs or cellular telephones (radio communications always take priority).
(2) Department cellular telephones or MCDs are intended to provide a means for employees to communicate *necessary official Department information* when other means are unavailable or the use would be inappropriate.
(3) Employees shall not use the cellular telephone in place of regular land-line telephone service for normal work functions.
(4) Any use of an MCD should be limited and clearly related to operational necessity. Audits of personal and Department-issued device use may be conducted at the Department's discretion. Department-issued MCDs may not be used in off-duty capacities; they are only for the conduct of law enforcement-related business or during Department-related off-duty law enforcement assignments.

(e) **Cellular Telephone Use While Driving/Moving.** When possible and practical, employees should pull their vehicle off the road and come to a complete stop prior to using Department cellular telephones or other MCDs, unless hands-free operational devices are authorized and available.

(f) **Records.** The records of MCD use, whether Department-owned or personal, while Officers are on duty may be subject to review by the Department.

(g) **Use of Audio and Visual Recordings.**

(1) Voice, text or image recordings obtained during the course and scope of employment, whether by personal or Department-issued equipment, are the property of the Department, and are governed by evidentiary policies of the Department, potential *Brady* disclosure requirements, and the Wisconsin Open Records Law.
(2) Audio recordings of conversations may be subject to federal and state wiretapping laws.
(3) The use of personal audio or video recording equipment, when such use is authorized by the Department, may be used to preserve perishable evidence when other options are not reasonably available. Officers shall make the Chief of Police aware of any recorded information that is obtained during the course and scope of the Officer's employment or that may be reasonably considered germaine to an investigation or other Department business.
(4) No Officer may erase, or attempt to alter, remove, or delete any audio, video or image related to Department business or taken while on duty from an MCD unless authorized to do so by the Department.

(5) Officers shall not keep personal copies of any image, audio or visual file related to Department business.

(6) Text, voice or photographic images made in the course of conducting law enforcement business, whether off or on duty, may not be shared with third parties in this Department or elsewhere, unless they have an official need and a right to such information in order to further an investigation or conduct other official Department business.

(7) Department members shall not use MCDs to share messages or visual/audio recordings with social or other print or electronic media, when such communications could reasonably be considered positions of the Department by others, could undermine Department integrity, or bring disrepute to the Department or its members.

DEFINITIONS:

(a) **Course/Scope of Employment.** Employee work or actions, whether performed on- or off-duty, to further the Department's law enforcement goals and responsibilities.

(b) **Disruptive Activity.** Any time that MCDs would be considered disturbing, such as in meetings, training sessions, court, or public places when their use would reasonably be deemed inappropriate or intrusive.

(c) **Distraction.** Any time the use of an MCD would divert, hinder, or delay the attention of an Officer from official duties and/or cause a potentially hazardous or unsafe situation.

(d) **Mobile Communication Device (MCD).** Cellular telephone, personal digital assistant (PDAs) and any such device designed to record, transmit, and/or receive voice communications, text messages, email, sound, video, or photographic images.

(e) **Personal Use.** Use of an MCD, to include but not be limited to, verbal conversations, texting, internet use, game playing, and similar functions that are unrelated to a Department member's employment.

COMMENTARY:

When Officers are interrupted and engaged in personal telephone calls while they are on patrol, they are distracted from and neglecting their official duties. When an Officer is engaged in official duties and his/her telephone rings, the distraction can cause a dangerous situation to occur, and an injury may occur because the Officer way not fully paying attention or because of the interruption involved in retrieving and answering a personal cellular telephone or pager. Officers may have many family members, friends, etc., who might have the Officer's cellular telephone number. If family members, friends, etc., call a Department employee when he/she

is on duty and supposed to be engaged in official duties, work productivity suffers, potential safety issues are significantly heightened, and a non-professional work image is presented to the public. Therefore, employees are to use extreme caution and good judgment when using personally owned cellular telephones in their possession while on duty with the Department.

Sec. 6-6-7 Employee Personal Internet Accounts.

POLICY:

(a) The Wisconsin Social Media Protection Act ["Act"], found in Sec. 995.55, Wis. Stats., protects individuals from invasive searches for private social media content by employers.

(b) The City of Stanley Police Department will administer its personnel relations with Department employees and prospective employees in accordance with the provisions of the Act. The restrictions in the Act apply to employers, educational institutions, and landlords.

(c) The Act creates two (2) basic restrictions on employers, which apply both to current employees and job applicants:

(1) The Act prohibits an employer from directly or indirectly accessing an individual's private social media content; and
(2) The Act prohibits an employer from retaliating against an individual for asserting rights under the Act.

(d) Employees who participate in the Department's hiring process, such as candidate interviews, may not request access to or review an applicant's social media profile while the individual remains in consideration for employment with the Department. This includes accepting or submitting "friend" requests on Facebook. The Department will take steps to ensure that permissible social media account information will be reviewed by a Department member who is not a decision-maker in the employment process. Such search results reported to the Department decision-maker will only be limited to information strictly relevant to the employment matter and are not of a discriminatory nature.

DEFINITIONS:

(a) **Access Information.** A user name and password or any other security information that protects access to a personal account.

(b) **Personal Internet Account.** An internet-based account that is created and used by an individual exclusively for purposes of personal communication.

PROCEDURES:

(a) There are no restrictions under the Act on viewing or accessing internet information about an individual that can be obtained in the public domain. The Act only protects information that an individual has taken steps to keep private.

(b) The Department may require a Department employee to disclose information to access an internet device, account or service if the Department provides the device, account or service to the employee. While this exception under the Act allows access to a smart-phone, computer or tablet that the Department provides to an employee, a personal social media account, as opposed to a Department account, accessed through the Department-furnished device is still protected under the Act and can be kept private by the employee.

(c) The Act contains several employer-specific exceptions to its general access limitations:

(1) A supervisory Officer of the Department may "friend" employees on Facebook without violating the Act, provided that "friend" inquiries or requests are prohibited if employment is conditioned on complying with the inquiry or request.

(2) The Act does not prohibit the Department as an employer from:

a. Disciplining or terminating a Department employee for transferring confidential, proprietary, or financial information of the Department to an employee's social media account.

b. Restricting employee access to certain internet sites on a Department computer, device or network.

c. Screening or monitoring that is required under federal or state law.

d. Requesting or requiring an individual to disclose his or her personal email address to facilitate communications.

e. Reviewing by the Department, as an employer, of private content to investigate suspected misconduct that occurs through social media. Importantly, however, an employer under the Act must first establish that it has reasonable cause to believe employment-related misconduct occurred before gaining extended-review privileges. Although an employer may investigate when there is reasonable cause to do so, the information being sought from a protected social media account must be limited – an investigating employer may only require an employee to grant access to or allow the employer to review or observe the employee's individual social media account. Employers are still restricted from asking for the login and password information on the account. Because the Act does not

define "reasonable cause", the employer should document its basis for believing reasonable cause exists (examples: public social media postings; information volunteered by an employee or given volutarily in the course of an employment interview). Once reasonable cause is believed to be established for Department supervisors to review an employee's private social media content, the scope of the employer's investigation still are limited. The Act only allows an investigating employer to then request that the employee login to the individual's private account for the employer to review or for the employer to observe while the employee navigates the account.

(3) Enforcement procedures for employer violations of the Act are handled by the Wisconsin Department of Workforce Development and are similar to investigations, hearings and procedures under the Wisconsin Fair Employment Act and Wisconsin Fair Housing Act.

(d) Besides the Act, other federal and state laws may also govern aspects of access to the social media accounts of employees, and the use of such information:

(1) Publicly available information on social media might relate to an employee's protected-class status under equal opportunity laws, such as the Wisconsin Fair Employment Act [Sec. 111.31-395, Wis. Stats.], Title VII of the Civil Rights Act of 1964 [42 U.S.C. 2000e-2000e-17], Americans with Disabilities Act [42 U.S.C. 12101-12213], and the Age Discrimination in Employment Act [29 U.S.C 621-634]. For example, an employee might post for public viewing photographs of his or her marriage or domestic partnership registration with a same-sex partner. If an employer made the decision not to hire that individual because of that person's sexual orientation, which the employer discovered through a review of information in the public domain, that decision would be unlawful discrimination under the Wisconsin Fair Employment Act. Although voluntary "friending" is permissible under the Act, the information an employment supervisor or decision-maker might learn related to an individual in a protected-class category may be cause to prohibit certain individuals from accepting or submitting friend requests to lower level employees.

(2) The federal Stored Communications Act [18 U.S.C 2701-2712] contains certain prohibitions against accessing electronic communications without authorization or exceeding authorization to access electronic communications; this federal law applies to anyone accessing an individual's social media or personal email account.

(3) The National Labor Relations Board (NLRB) also can scutinize how employers regulate employee social media use in a manner which might violate the National Labor Relations Act and associated union activities. For example, something that could be examined by the NLRB is employees' discussion of working conditions on social media and employer responses.

Title 6 ▸ Chapter 7

Communications Procedures

Sec. 6-7-1 Radio Traffic Conduct.

POLICY:

Radio traffic shall:

(a) Be brief on conversation.

(b) Engage in radio conversation that pertains only to official business.

(c) Maintain radio system discipline.

COMMENTARY:

Radio traffic shall be responsible, efficient and courteous. City of Stanley Police Department members engaged in radio traffic should exercise extreme courtesy and extend maximum consideration, understanding and cooperation to both the public and the members of the Department. They must recognize that in many cases they will be the first and, in some instances, the only law enforcement contact by many citizens and that good or bad impressions thus gained will influence the attitude of the citizens toward the police.

Sec. 6-7-2 Radio Etiquette.

POLICY:

(a) All Officers of the City of Stanley Police Department shall become acquainted with correct radio operation and procedures.

(b) All Officers, when using the radio, shall speak in a loud and clear voice so the operator and other units can understand the Officer the first time without repeating the message again. All radio conversations shall be limited to law enforcement business only. At no time shall an Officer use insulting language or conduct business via the radio. Further, Officers shall not make derogatory remarks about complaints, citizens or fellow employees.

(c) Officers should realize that their radios are constantly being monitored by citizens of the community and shall be guided accordingly in their conversations. Recorded tapes, if available, will be monitored periodically to see if Officers use proper procedures.

(d) Officers shall not use the police radio except for official police communications. At no time shall an Officer use discourteous, obscene or disrespectful language during the transmission of a radio message.

(e) Officers shall keep their radios turned on and tuned to the local band unless instructed otherwise or if on a special assignment. Before an Officer leaves his/her vehicle, he/she should give his/her location where he/she can be reached, which shall be acknowledged by the Communications Center.

(f) Whenever an assignment is completed, Officers shall use the proper code word.

Title 6 ▸ Chapter 8

Laptop/Mobile Data Computer Use

Sec. 6-8-1 Laptop/Mobile Data Computer Use.

POLICY:

(a) The purpose of this Chapter is to establish standard procedures and policies for the use of Department Laptop/Mobile Date Computers ("laptop"), to set forth rules governing their use, and to define the responsibilities of Officers and supervisory personnel when using this equipment, as well as informing users of the impact of the Open Records Law regarding laptop communications.

(b) The Laptop/Mobile Data Computer ("laptop") shall be used to enhance and support radio communications. The laptop is not to be considered the primary source of communication between the Officer in the field and Communications Center personnel. Proper use of the laptop will reduce unnecessary radio traffic, provide the transfer of information in a secure method and allow the Officer, in the field, to better utilize available resources.

(c) Laptops/mobile data computers, in addition to being a Windows-compatible computer system, are fully functional radio transmitters and receivers operating in the 800 MHz radio range. As such, this equipment is subject to regulations of the State of Wisconsin as well as the Federal Communications System (FCC).

(d) It is the policy of this Department to utilize radio and laptop communications in a professional and efficient manner. FCC and State rules ban unnecessary or superfluous communications. The Department member using a Department laptop shall be personally responsible for the proper and safe use of this equipment. The user of this equipment is capable of broadcasting open text messages to single units or to the Communications Center. All messages shall be limited to duty-related business. Under no circumstances

shall a Department member using this equipment transmit messages that contain jokes, sexual comments or innuendoes of a provocative, suggestive or racist nature.

Sec. 6-8-2 Restrictions on Use of Laptops/Mobile Data Computers.

POLICY:

(a) Communications over Department laptops/mobile data computers ("laptops") shall be limited exclusively to official Department business and shall be done in a professional manner. Indecent or profane language is strictly prohibited.

(b) Only authorized City of Stanley Police Department employees shall be authorized and permitted to use Department laptops.

(c) All Department members may be required to be TIME certified before using any Department laptop/mobile data computer.

(d) Officers shall give due consideration to proper driving techniques and shall avoid, when possible, typing messages or use of the laptop during the operation of a vehicle.

Sec. 6-8-3 Proper Use of Laptops/Mobile Data Computers.

PROCEDURES:

(a) Officers who log in on the terminal at the beginning of the shift shall log off at the completion of their shifts.

(b) Officers are able to access WisDOT and CIB records through the TIME system, via the laptop. Generally, Officers will run their own checks. If safety or accessibility become a factor, the checks can be run through the Communications Center. Officers may have the Communications Center run inquiries whenever the readout is confusing.

(c) If an Officer determines from CIB via the laptop that a particular person is wanted on an outstanding warrant or other type of hold, the warrant or hold will have to be confirmed with the agency involved. This cannot be done directly from the squad vehicle via the laptop. The Officer will have to notify a telecommunicator at the Communications Center who in turn will have to send a confirmation request to the agency involved. Officers shall have the Communications Center re-run any wanted person data and confirm the status of the individual with the appropriate agency.

(d) When dealing with laptop responses on wanted persons, the Officer should be mindful of the geographic restrictions found on many wanted entries. These restrictions limit where the warrant is valid. They include county of the originating agency only and, in some cases, adjacent counties only. It is the Officer's responsibility to determine if the warrant or hold is valid in the Department's jurisdiction by use of these "limiter" messages. This determination should be made prior to requesting a telecommunicator to confirm the warrant through the originating agency.

(e) Officers who are checking out of the squad vehicle for warrant service, checking for a wanted person, or when they believe that an arrest may result from the situation shall communicate such over the radio.

(f) Generally, complaints shall be dispatched and acknowledged over the radio. Communications during tactical events or information of a sensitive nature that may be inappropriate to broadcast over the radio shall be transmitted by use of the laptop. Officers are required to keep all Department personnel informed of these situations.

(g) Officers shall retain the discretion to use radio transmissions in lieu of the laptop in circumstances when the facts/situation indicate the use of the laptop would jeopardize the Officer's safety.

Sec. 6-8-4 Laptop Messages and the Open Records Law.

The Wisconsin Open Records Law essentially states that any record generated by government must be preserved and be available for public inspection upon appropriate request. Messages sent from Department laptops as well as radio voice communications fall within the category of "records" for the purposes of this law. Every message sent via Department laptops shall be recorded and maintained by the Communications Center. Likewise, messages received by WisDOT and CIB data bases are saved to an audit trail. All voice communications are recorded. These "records" are available for public inspection upon request.

Title 6 ▸ Chapter 9

Hearing Impaired/Disabled Communications

Sec. 6-9-1 Communications Considerations.

POLICY:

(a) **Purpose and Scope.** Individuals who suffer from deafness, hearing impairment, blindness, impaired vision, mental or other disabilities may encounter difficulties in gaining meaningful access to, or an understanding of important rights, obligations and services. In accordance with the federal Americans with Disabilities Act (ADA), it is therefore the policy of the City of Stanley Police Department to take all reasonable steps to accomodate such individuals in any law enforcement contact.

(b) **Factors to Consider.**

(1) Because the nature of any law enforcement contact may vary substantially from one situation to the next, employees of this Department should consider all information reasonably available to them when determining how to communicate with an individual suffering from any disability. These factors may include, but are not limited to:

a. The extent to which a disability is obvious or otherwise made known to the involved employee. Impaired or disabled individuals may be reluctant to acknowledge their condition and may even feign a complete understanding of a communication despite actual confusion.
b. The type of disability (e.g., total deafness or blindness vs. impairment).
c. The nature of the law enforcement contact (e.g., emergency vs. non-emergency, custodial vs. consensual contact, etc.).
d. Availability of resources to aid in communication.

(2) When considering these factors and other available information, the involved employee(s) should carefully balance all factors in an effort to reasonably ensure meaningful access by individuals suffering from apparent disabilities to critical services while not imposing undue burdens on the Department and its Officers.

(c) **Initial and Immediate Considerations.** Recognizing that various law enforcement encounters may be potentially volatile and/or emotionally charged, Department employees should remain alert to the possibility of communications problems and exercise special care in the use of all gestures, and verbal and written communication in an effort to minimize initial confusion and misunderstanding when dealing with any individual(s) with known or suspected disabilities or communications impairments.

Sec. 6-9-2 Types of Assistance Available.

POLICY:

Depending on the balance of factors available for consideration at the time, the Department will make every reasonable effort to provide meaningful and timely assistance to disabled individuals through a variety of services, where available. Disabled individuals may elect to accept such assistance at no cost, choose to provide their own communication services at their own expense, or any combination thereof. In any situation, the individual's expressed choice of communication method shall be given primary consideration and honored unless the employee can adequately demonstrate that another effective method of communication exists under the circumstances.

PROCEDURES:

Officers should document the type of communication utilized in any related report and whether a disabled or impaired individual elected to use services provided by the Department or some other identified source. Department-provided services may include, but are not limited to, the following:

(a) **Field Resources.** Individual Officers and employees of the Department are encouraged to utilize resources immediately available to them in any contact with a known or suspected disabled or impaired person. Examples of this would include such simple methods as:
(1) Hand gestures or written communications exchanged between the employee and a deaf or hearing impaired individual.
(2) Facing an individual utilizing lip reading and speaking slowly and clearly.
(3) Slowly and clearly speaking or reading simple terms to any visually or mentally impaired individual.

(b) **Audio Recordings and Enlarged Print.** From time to time, the Department may develop audio recordings of important information needed by blind or visually impaired individuals. In the absence of such audio recordings, employees may elect to read aloud a Department form or document (such as a citizen complaint form) to a visually impaired individual or utilize a photocopier to enlarge printed forms for a visually impaired individual.

(c) **Telephone Interpeter Services.** The Department will attempt to maintain a list of qualified interpreter services to be contacted at Department expense to assist deaf or hearing impaired individuals upon approval of the Chief of Police. When utilized, notification to such interpreters shall be made at the earliest reasonable opportunity and the interpreter should be available to respond within a reasonable time [generally not to exceed three (3) hours].

(d) **TTY and Relay Services.** Individuals who are deaf or hearing impaired must be given the opportunity to use available text telephones (TTY or TDD). All calls placed by such individuals through such services shall be accepted by this Department.

(e) **Community Volunteers.** Depending on the circumstances, location and availability, responsible members of the community may be available to provide qualified interpreter services, such as those who are proficient in American Sign Language (ASL). Sources for these individuals may include local businesses, banks, churches, neighborhood leaders and school district officials. In addition to such sources developed by individual Officers, the Department will attempt to maintain and update a list of qualified volunteers who may be available to respond within a reasonable time.

(f) **Family and Friends of Disabled or Impaired Individual.** While family and friends of a disabled or impaired individual may frequently offer to assist with interpretation, employees should carefully consider the circumstances before relying on such individuals. For example, children should not be relied upon except in emergency or critical situations. Further, the nature of the contact and relationship between the disabled individual and the individual offering services must be carefully considered (e.g., victim/suspect).

Sec. 6-9-3 Contact Situations and Reporting.

POLICY:

While all contacts, services, and individual rights are important, the Department will carefully consider reasonably available information in an effort to prioritize services to disabled and impaired individuals so that such services and resources may be targeted where most needed because of the nature and importance of the particular law enforcement activity involved.

PROCEDURES:

(a) **Reports.** Whenever any member of the Department is otherwise required to complete a report or other documentation, and communication assistance is provided to any individual disabled or impaired individual, such services should be noted in the related report.

(b) **Receiving and Responding to Requests for Assistance.**

(1) In order to provide disabled and impaired individuals with meaningful access to law enforcement services when they are victims of, or witnesses to, alleged criminal activity or other emergencies, the Department has designated working with the 911 Communications Center as a top priority with such services. Department personnel will make every reasonable effort to promptly accomodate such disabled and impaired individuals utilizing 911 communications through any or all of the above resources.

(2) While 911 dispatches received by the Department shall receive top priority, it is also important that reasonable efforts be made to accomodate such disabled and impaired individuals seeking more routine access to services and information from the Department.

(c) **Custodial Interrogations and Bookings.**

(1) In an effort to ensure that the rights of all disabled and impaired individuals are protected during arrest and custodial interrogation, the Department places a high priority on providing reasonable communication assistance during such situations. It is further recognized that miscommunication during custodial interrogations may have a substantial impact on the evidence presented in any related criminal prosecution. As such, Department personnel providing communication assistance in these situations will make every reasonable effort to accurately and effectively communicate with disabled or impaired individuals.

(2) Employees providing such assistance shall also be aware of the inherent communication impediments to gathering information from disabled or impaired individuals throughout the booking process or any other situation in which a disabled or impaired individual is within the control of Department personnel. Medical screening questions are commonly used to elicit information on individual's medical needs, suicidal inclinations, presence of contagious diseases, potential illnesses, resulting symptoms upon withdrawl from certain medications, or the need to segregate the arrestee from other prisoners, therefore it is important for this Department to make every reasonable effort to provide effective communication assistance in these situations.

(3) Individuals who require communication aids, such as hearing aids, should be permitted to retain such devices while in custody.

(4) While it may present Officer safety issues or other logistical problems to allow a physically disabled individual to retain devices such as a wheel chair or crutches during a custodial situation, the removal of such items will require that other reasonable accomodations be made to assist such individuals with access to all necessary services.

(5) Whenever a deaf or hearing imparied individual is detained or arrested and placed in handcuffs, Officers should consider, safety permitting, placing the handcuffs in front of the body in order to allow the individual to sign or write notes.

(d) **Field Enforcement and Investigations.**

(1) Field enforcement will generally include such contacts as traffic stops, pedestrian stops, serving warrants and restraining orders, crowd/traffic control and other routine field contacts which may involve disabled or impaired individuals. The scope and nature of these activities and contacts will inevitably vary, therefore the Department recognizes that it would be virtually impossible to provide immediate access to complete communication services to every Officer in the field. Each Officer and/or supervisor must, however, assess each such situation to determine the need and availability for communication assistance to any and all involved disabled or impaired individuals.

(2) Although not every situation can be addressed within this policy, it is important that Department employees are able to effectively communicate the reason for a contact, the need for information and the meaning or consequences of any enforcement action taken with a disabled or impaired individual. For example, it would be meaningless to verbally request consent to search if the Officer is unable to effectively communicate with a deaf individual.

Sec. 6-9-4 Training.

PROCEDURES:

In an effort to ensure that all Department employees in public contact positions (or having contact with those in custody) are properly trained, the Department will provide periodic training in the following areas:

(a) Employee awareness of related policies, procedures, forms and available resources.

(b) Employees having contact with the public (or those in Department custody) are trained to work effectively with in-person and telephone interpreters and related equipment.

(c) Training and/or providing educational materials for Department members in a supervisory capacity, even if they may not interact regularly with disabled individuals, in order that they may remain fully aware of, and understand these policies and procedures, so that Department members can reinforce its importance and ensure its implementation by staff.

Title 6 ▸ Chapter 10

Limited English Proficiency Services

Sec. 6-10-1 Purpose and Scope; Definitions.

POLICY:

Language barriers can sometimes inhibit or even prevent individuals with limited English proficiency (LEP) from gaining meaningful access to, or an understanding of, important rights, obligations and services. It is the policy of the City of Stanley Police Department to take reasonable steps to ensure timely and equal access to services by all individuals, regardless of national origin or primary language. [Title VI of the Civil Rights Act of 1964, Sec. 601, 42 United States Code 2000d].

DEFINITIONS:

The following definitions shall be applicable in this Chapter:

(a) **Limited English Proficient/Proficiency (LEP).** Individuals whose primary language is not English and who have a limited ability to read, write, speak, or understand English. LEP individuals may be competent in certain types of communications (e.g., speaking or understanding), but still be LEP classified for other purposes (e.g., reading or writing). LEP designations are context-specific – an individual may possess sufficient English language skills to function in one setting, but these skills may be insufficient in other situations.

(b) **Interpretation.** The act of listening to a communication in one language ("source language") and orally converting it to another language ("target language") while retaining the same meaning.

(c) **Translation.** The replacement of written text from one language ("source language") into an equivalent written text ("target language").

(d) **Bilingual.**

(1) The ability to communicate in two (2) languages fluently, including the ability to communicate technical and law enforcement and criminal justice terminology. Bilingual includes a variety of skill levels. For example, some bilingual individuals may be fluent enough to engage in direct communications in a non-English language, but are insufficiently fluent to interpret or translate from one language to another. For example, a bilingual individual, depending on his/her skill level, could be utilitzed to communicate fluently in a non-English language, but not to interpret between two (2) languages if he/she does not possess the specialized skills necessary to interpret between two (2) languages effectively.

(2) In order to be utilized to interpret or translate from one language into another, an individual must possess the skill, training and demonstrated competence to do so. For purposes of this Chapter, Department members, in order to be identified as bilingual, must initially and periodically demonstrate, through a procedure approved by the Chief of Police, their level of skill and competence such that the Department is able to determine the purposes for which an employee's language skills may be used.

(e) **Authorized Interpreter.** A member of the Department, a member of another law enforcement agency, or a professional in the employ of the Department who is bilingual and has successfully completed Department-prescribed interpreter training and is authorized to act as an interpreter or translator.

Sec. 6-10-2 Four Factors Analysis in LEP Situations.

POLICY:

(a) **U.S. Justice Department's Analysis Approach.** Since there are potentially hundreds of languages Department personnel could encounter, the City of Stanley Police Department will make a reasonable attempt to utilize the four (4) factors analysis outlined in the U.S. Department of Justice LEP *Guidance to Federal Financial Assistance Recipients* in determining which measures will provide reasonable and meaningful access to various rights, obligations, services and programs to the general public.

(b) **Balancing Four Factors in LEP Situations.** It is recognized that law enforcement contacts and circumstances will vary considerably. The utilization of the four (4) factors analysis must therefore be flexible, with Department members striving for an ongoing balance of the following four (4) factors:

(1) ***Factor 1 – Demographics of Service Area.*** The number of or proportion of LEP individuals likely to be served or who are likely to be encountered by Department personnel or who may benefit from programs or services within this Department's jurisdiction or a particular geographic area.

(2) ***Factor 2 – Frequency of Contact with Law Enforcement Personnel.*** The frequency with which LEP individuals are likely to become in contact with personnel, programs and/or services of the Department.

(3) ***Factor 3 – Type and Importance of Contacts.*** The nature, type and importance of the contact, program, information, and/or service(s) provided by the Department.

(4) ***Factor 4 – Cost and Available Resources.*** The cost of providing LEP assistance and the resources available to the Department.

(c) **Policy Goal of the Four Factors Analysis.** For the reasons explained above, the intent of the four (4) factors analysis is to provide a balance that reasonably ensures meaningful access by LEP individuals to critical services while not imposing undue or unreasonable burdens on the Department and its personnel given limited resources.

(d) **Services Determination.** While the Department will not discriminate against or deny any individual access to services, rights or programs based upon national origin or any other protected interest or right, the above four (4) factors analysis will be utilized by the Department to determine the availability and level of assistance that can be provided to any LEP individual or group.

(e) **Identification of LEP Individual's Language.** The Department will utilize reasonably available tools, such as language identification cards, when attempting to determine a LEP individual's primary language in an effort to avoid misidentifying that language.

Sec. 6-10-3 LEP Assistance Available.

PROCEDURES:

(a) **Types of LEP Assistance Available.**

(1) Depending on the balance of the four (4) factors outlined in Sec. 6-10-2 above, the Department will make every reasonable effort to provide meaningful and timely assistance to LEP individuals through a variety of services, where available. LEP individuals may elect to accept interpreter services offered through the Department at no cost or choose to provide their own interpreter/translator services at their own expense.

(2) Department personnel should document in any related report whether the LEP individual elected to use interpreter services provided by the Department or some other source. Department-provided interpreter/translator services may include, but are not limited to, the assistance methods described below in this Section.

(b) **Bilingual Staff.**

(1) Employees utilized for providing LEP services need not be certified as interpreters, but must have demonstrated a level of competence to ascertain whether the employee's language skills are best suited to monolingual communications, interpretation, translation, or all or none of these functions. All employees used for communication with LEP individuals must demonstrate knowledge of the ethical issues involved when functioning as a language conduit.

(2) In addition, employees who serve as interpreters and/or translators must have demonstrated competence in both English and the non-English language involved and knowledge of the functions of an interpreter, including, but not limited to, the ethics requirements of interpretation.

(3) When bilingual employees of this Department are not available, employees from other departments who have the requisite training may be requested.

(c) **Written Forms and Guidelines.** The Department will make a reasonable effort to identify the most frequently used and critical forms and guidelines and translate these documents into the languages most likely to be requested. The Department will try to arrange to make translated forms available to Department personnel and other appropriate individuals.

(d) **Audio Recordings.** From time to time, the Department may develop audio recordings of important information needed by LEP individuals for broadcast in a language most likely to be understood by involved LEP individuals.

(e) **Telephone Interpreter Services.** The Chief of Police will make reasonable efforts to maintain a list of qualified interpreter services which can be contacted to assist LEP individuals by telephone.

(f) **Community Volunteers and Other Sources of Interpretation.**

(1) Where competent bilingual Department personnel or other City staff are unavailable to assist, responsible members of the community who have demonstrated competence in either monolingual (direct) communication and/or in interpretation and translation [as noted in Subsection (b) above] may be called upon to assist in communication efforts. Sources for these individuals may include neighoring law enforcement

agencies, school officials and languages instructors, local businesses, churches, and neighborhood leaders. Department personnel should ensure that community members are able to provide unbiased assistance. The nature of the contact and relationship between the LEP individual and the person offering services must be carefully considered by Officers (e.g. victim/suspect).

(2) Except for exigent or very informal and non-confrontational circumstances, the use of an LEP individual's bilingual friends or family members, particularly children, is generally not recommended and Department personnel shall make case-by-case determinations on the appropriateness of using such individuals.

Sec. 6-10-4 LEP Contact Situations and Reporting.

POLICY:

(a) **Generally.**

(1) While all law enforcement contacts, services and individual rights are important, the Department will utilize the four (4) factors analysis to prioritze language services so that they may be directed where they are most needed.

(2) Whenever any member of the Department is required to complete a report or other documentation and interpretation or translation services are provided to any involved LEP individual, such services should be noted in any related reports.

(b) **Receiving and Responding to Requests for Assistance.**

(1) In order to provide LEP individuals with meaningful access to law enforcement services when they are victims of, or witnesses to, alleged criminal activity or other emergencies, Department personnel will make reasonable efforts to promptly accommodate such LEP individuals when 911 calls for assistance are received.

(2) While 911 calls for assistance shall receive top priority, it is also important that reasonable efforts be made to accommodate LEP individuals seeking more routine access to services and information from the Department by utilizing all the methods listed in Sec. 6-10-3 above.

(c) **Field Enforcement and Investigations.**

(1) Field enforcement generally will include such contacts as traffic stops, pedestrian stops, serving warrants and restraining orders, traffic/crowd control, and other routine field contacts which may involve LEP individuals. The scope and nature of these

activities and contacts will inevitably vary. Department personnel must assess each situation to determine the need and availability for translation services to all involved LEP individuals and utilize the methods outlined in Sec. 6-10-3 to provide appropriate language assistance.

(2) Although not every situation can be addressed within this Chapter, it is important that Department personnel are able to effectively communicate the reason for a contact, the need for information and the meaning or consequences of any enforcement action taken with an LEP individual. It would, for example, be meaningless to request consent to search if the person requesting is unable to effectively communicate with an LEP individual.

(d) **Investigative Interviews.**

(1) In any situation where the translation of an interview may contain information that might be used in a criminal trial, it is important to take certain steps to improve the chances of admissibility. This includes interviews conducted during an investigation with victims, witnesses and suspects. In such situations, audio recordings of the interviews should be made when reasonably possible. Identifying and contact information for the interpreter, such as name and address, should be documented so that the person can be subpoenaed for trial if necessary.

(2) Any person selected as an interpreter and/or translator must have demonstrated competence in both English and the non-English language involved and knowledge of the functions of an interpreter that allows for correct and effective translation and should not be a person with an interest in the case. The person providing interpretation or translation services may be required to establish the accuracy and trustworthiness of the interpretation or translation to the court.

(e) **Custodial Interrogations and Bookings.**

(1) In an effort to ensure that the rights of LEP individuals are protected during arrest and custodial interrogation, the Department places a high priority on providing competent interpretation during such situations. It is further recognized that miscommunication during custodial interrogations may have a substantial impact on the evidence presented in any related criminal prosecution. As such, Department personnel providing interpretation services or translated forms in these situations must have demonstrated competence in interpretation/translation and make every reasonable effort to accurately interpret/translate all communications with LEP individuals.

(2) In order to ensure that translations during criminal investigations are documented accurately and admissible as evidence, audio recordings of interrogations, victim interviews and witness interviews should be used whenever reasonably possible.

(3) Employees providing translation services shall also be aware of the inherent communication impediments to gathering information from the LEP individual throughout the booking process or any other situation in which an LEP individual is within the control of Department members. Medical screening questions, for example, are commonly used to elicit information on individual's medical needs, suicidal inclinations, presence of contagious diseases, potential illnesses, resulting symptoms upon withdrawl from certain medications, or the need to segregate the arrestee from other prisoners; it is important for Department members to make reasonable efforts to provide effective language services in these situations.

(f) **Complaints.** The Department will ensure access to LEP persons who wish to file a complaint regarding the discharge of Department duties and the provision of services. The Department may do so by providing interpretation assistance or translated forms to such individuals. The Department will make reasonable attempts to communicate its response(s) in an accessible manner.

(g) **Community Outreach.** Community outreach programs have become increasingly recognized as being important to the success of more traditional law enforcement duties. The Department will work with community groups, local businesses and neighborhoods to provide equal access to such programs and services to LEP individuals and groups.

Sec. 6-10-5 Training.

POLICY:

The City of Stanley Police Department will make reasonable efforts to provide periodic training resources to personnel about Department LEP policies and procedures, including how to access authorized interpreters, translators, and other available resources.

Sec. 6-10-6 Interpreters and Translators; Supplemental Materials.

POLICY:

(a) **Skills Assessment.**

(1) Department members and other persons identified as having the skills or training to interpret, translate or provide language assistance will have their language proficiency assessed by a professional approved by the Chief of Police. An interpreter/translator

must demonstrate proficiency in and ability to communicate information accurately in both English and in the target language, have knowledge in both languages of specialized terms used by the LEP person, and understand and adhere to the interpreter/translator role without deviating into other roles such as counselor or legal advisor.

(2) The Chief of Police will try to keep the Authorized Interpreters/Translators List current.

(b) **Supplemental Materials.** The Department will make reasonable efforts to make the following materials available to Department members to assist in providing access and services to LEP individuals:

(1) Listing of Department bilingual employees, language spoken, contact information, and general shift information.
(2) Listing of Department-approved interpretation/translating services, including names of bilingual interpreters/translators, languages spoken, contact information, and availability information.
(3) Telephone number and any access code information of telephonic interpretation services.
(4) Language identification cards.
(5) Translated *Miranda* warning cards and other frequently-used translated documents in the language(s) most likely to be encountered (e.g. Spanish).
(6) Any audio recordings/warnings that are developed by the Department in non-English languages.

Title 6 ▸ Chapter 11
Portable Audio/Video Recorders

Sec. 6-11-1 Portable Audio/ Video Recorders.

PURPOSE AND SCOPE:

This policy provides guidelines for the use of portable audio/video recording devices by members of this department while in the performance of their duties. Portable audio/video recording devices include all recording systems, whether body-worn, hand-held, or integrated into portable equipment (Wis. Stat. § 165.87).

This policy does not apply to mobile audio/video recordings, interviews, or interrogations conducted at any Stanley Police Department facility, authorized undercover operations, wiretaps, or eavesdropping (concealed listening devices).

POLICY:

The Stanley Police Department may provide staff with access to portable recorders, either audio or video or both, for use during the performance of their duties. The use of recorders is intended to enhance the mission of the Department by accurately capturing contacts between members of the Department and the public.

STAFF PRIVACY EXPECTATION:

All recordings made by members on any department-issued device at any time, and any recording made while acting in an official capacity of this department regardless of ownership of the device it was made on, shall remain the property of the Department. Staff shall have no expectation of privacy or ownership interest in the content of these recordings.

STAFF RESPONSIBILITIES:

Prior to going into service, each officer will be responsible for making sure that he/she is equipped with a portable recorder issued by the Department, and that the recorder is in good working order. If the recorder is not in working order or the member becomes aware of a malfunction

malfunction at any time, the member shall promptly report the failure to the Chief of Police and obtain a functioning device as soon as reasonably practicable. Uniformed members should wear the recorder in a conspicuous manner or otherwise notify persons that they are being recorded, whenever reasonably practicable.

Any member assigned to a non-uniformed position may carry an approved portable recorder at any time the member believes that such a device may be useful. Unless conducting a lawful recording in an authorized undercover capacity, non-uniformed members should wear the recorder in a conspicuous manner when in use or otherwise notify persons that they are being recorded, whenever reasonably practicable.

ACTIVATION OF THE AUDIO/VIDEO RECORDER:

This policy is not intended to describe every possible situation in which the portable recorder should be used, although there are many situations where its use is appropriate. Officers should activate the recorder any time they believe it would be appropriate or valuable to record an incident.

The portable recorder should be activated in any of the following situations:

(a) All enforcement and investigative contacts including stops and field interview situations

(b) Traffic stops including, but not limited to, traffic violations, stranded motorist assistance and all crime interdiction stops

(c) Self-initiated activity in which a member would normally notify dispatch

(d) Any other contact that becomes adversarial after the initial contact in a situation that would not otherwise require recording

Members should remain sensitive to the dignity of all individuals being recorded and exercise sound discretion to respect privacy by discontinuing recording whenever it reasonably appears to the member that such privacy may outweigh any legitimate law enforcement interest in recording.

Requests by members of the public to stop recording should be considered using this same criterion. Recording should resume when privacy is no longer at issue unless the circumstances no longer fit the criteria for recording.

At no time is staff expected to jeopardize his/her own safety in order to activate a portable recorder or change the recording media. However, the recorder should be activated in situations described above as soon as reasonably practicable.

CESSATION OF RECORDING:

Once activated, the portable recorder should remain on continuously until the member reasonably believes that his/her direct participation in the incident is complete or the situation no longer fits the criteria for activation. Recording may be stopped during significant periods of inactivity such as report writing or other breaks from direct participation in the incident.

SURREPTITIOUS USE OF THE PORTABLE RECORDER:

Wisconsin law permits an individual to surreptitiously record any conversation in which one party to the conversation has given his/her permission (Wis. Stat. § 968.31(2)(b)).

Members may surreptitiously record any conversation during the course of a criminal investigation in which the member reasonably believes that such a recording will be lawful and beneficial to the investigation.

Members shall not surreptitiously record another department member without a court order unless lawfully authorized by the Police Chief or the authorized designee.

EXPLOSIVE DEVICE:

Many portable recorders, including body-worn cameras and audio/video transmitters, emit radio waves that could trigger an explosive device. Therefore, these devices should not be used where an explosive device may be present.

PROHIBITED USE OF PORTABLE RECORDERS:

Staff is prohibited from using department-issued portable recorders and recording media for personal use and are prohibited from making personal copies of recordings created while on-duty or while acting in their official capacity.

Staff is also prohibited from retaining recordings of activities or information obtained while engaged in a law enforcement function, whether the recording was created with department-issued or personally owned recorders. Staff shall not duplicate or distribute such recordings, except for authorized legitimate department business purposes. All such recordings shall be retained at the Department.

Staff is prohibited from using personally owned recording devices to record while on-duty without the consent of the Chief of Police. Any member who uses a personally owned recorder for department-related activities shall comply with the provisions of this policy, including retention and release requirements, and shall notify the Chief of Police of such use as soon as reasonably practicable. Recordings shall not be used by any member for the purpose of embarrassment, harassment or ridicule.

IDENTIFICATION AND PRESERVATION OF RECORDINGS:

To assist with identifying and preserving data and recordings, members should download, tag or mark these in accordance with procedure and document the existence of the recording in any related case report.

A member should transfer, tag or mark recordings when the member reasonably believes:

(a) The recording contains evidence relevant to potential criminal, civil or administrative matters.

(b) A complainant, victim or witness has requested non-disclosure.

(c) A complainant, victim or witness has not requested non-disclosure but the disclosure of the recording may endanger the person.

(d) Disclosure may be an unreasonable violation of someone's privacy.

(e) Medical or mental health information is contained.

(f) Disclosure may compromise an undercover officer or confidential informant.

(g) The recording or portions of the recording may be protected under the Public Records Law (Wis. Stat. § 19.31 et seq.).

REVIEW OF RECORDED MEDIA FILES:

When preparing written reports, members may review their recordings as a resource. However, staff shall not retain personal copies of recordings. Staff should not use the fact that a recording was made as a reason to write a less detailed report.

The Chief of Police is authorized to review relevant recordings any time he/she is investigating alleged misconduct, or reports of meritorious conduct, or whenever such recordings would be beneficial in reviewing the member's performance. Recorded files may also be reviewed:

(a) Upon approval by the Chief of Police, by any member of the Department who is participating in an official investigation, such as a personnel complaint, administrative investigation, or criminal investigation.

(b) Pursuant to lawful process or by court personnel who are otherwise authorized to review evidence in a related case.

(c) By media personnel with permission of the Police Chief or the authorized designee.

(d) In compliance with a public records request, if permitted, and in accordance with the Release of Information Policy.

All recordings should be reviewed by the Chief of Police prior to public release. Recordings that unreasonably violate a person's privacy or sense of dignity should not be publicly released unless disclosure is required by law or order of the court (Wis. Stat. § 165.87(3)).

COORDINATOR:

The Police Chief or the authorized designee should designate a coordinator responsible for (Wis.Stat. § 165.87):

(a) Establishing procedures for the security, storage, and maintenance of data and recordings.

(b) Establishing procedures for accessing data and recordings.

(c) Establishing procedures for logging or auditing access.

(d) Establishing procedures for transferring, downloading, tagging, or marking events.

(e) Periodically reviewing the Department's practices relating to the use, maintenance, and storage of body cameras and data to confirm compliance with this policy.

RETENTION OF RECORDINGS:

All recordings shall be retained for a period consistent with the requirements of the established records retention schedule but in no event for a period less than 120 days (Wis. Stat. § 165.87).

EXCEPTIONS TO RETENTION REQUIREMENTS FOR BODY-WORN CAMERAS:

Exceptions to the 120-day retention period for body-worn cameras are as follows (Wis. Stat. § 165.87):

(a) Recordings should be retained until the final disposition of any investigation, case, or complaint to which the recordings pertain to any of the following:

1. Death or alleged physical injury to any person in the recording
2. An encounter resulting in custodial arrest
3. A search during a temporary detention pursuant to Wis. Stat. § 968.25
4. An encounter resulting in the use of force except when the only use of force involves the use of a firearm to euthanize an injured wild animal

(b) Recordings used in any criminal, civil, or administrative proceeding may not be destroyed except upon a final disposition from the court or hearing officer after a determination that the recordings are no longer needed, or by an order from the court or hearing officer.

(c) Recordings may be retained for a period beyond 120 days if a request or directive to preserve the recordings is made before the expiration of that time period by an officer from this department or another law enforcement agency, prosecutor, defendant, or a court.

RELEASE OF AUDIO/VIDEO RECORDINGS:

Requests for the release of audio/video recordings shall be processed in accordance with the Release of Information Policy (Title 6: Chapter 2)