

Computer and Internet Usage

Investigation and Discipline Guidelines

I.	Introduction.....	3
II.	Roles and Responsibilities	3
	A. Incident Response Person	4
	B. Supervisor	4
	C. Manager	4
	D. Human Resource Professional	4
	E. Information Technology Professional.....	5
III.	Incidents That Require Investigation	5
	A. Impermissible Activities	5
	B. Reporting Sources.....	6
IV.	Collecting Basic Information.....	6
	A. Getting Started	6
	B. Involving Law Enforcement Officials	7
V.	Determining the Scope of the Investigation.....	7
VI.	Obtaining Computer Evidence.....	8
	A. The Subject Employee	8
	B. Surveying the Workstation	8
	C. Handling the Hard Drive.....	10
	D. Other Sources of Evidence.....	10
VII.	Timing the Collection of Computer Evidence	11
	A. Seize the Computer Hardware/Software NOW – Option 1	11
	B. Obtain the Evidence LATER When Employee Is Not Present – Option 2	12
	C. Monitor and Obtain Evidence at a Later Date – Option 3	12
VIII.	Preserving Evidence (Chain of Custody).....	13
IX.	Technical Aspects of Hard Drive Evidence.....	13

X.	The Investigative Interview Process	14
	A. Interview Process	15
	B. Develop Questions	15
	C. Determine the order of the interview(s).....	16
	D. Conducting the Interviews	16
XI.	The Discipline Process.....	17
XII.	Post Investigation Activities	18
XIII.	Conclusion	19
XIV.	Resources	20

Disclaimer: This document is not intended to provide legal advice or to establish any specific contractual rights for employees.

I. Introduction

The purpose of this document is to discuss the best practices and procedures for supervisors, managers, and human resource offices to follow upon receipt of allegations of employee misuse and/or abuse of State owned e-mail, Internet systems and any and all software, data, or other information stored on a State owned computer. This includes unauthorized access to or dissemination of not public data. For purposes of these guidelines, “employees” includes consultants, contractors, and volunteers. Issues relating to the investigation of unauthorized activity by non-employees such as senders of malicious code, hackers, and crackers are outside of the scope of this resource.

While this document is not meant to be all-inclusive, it is intended to identify procedures that supervisors, managers, Human Resource professionals, and other involved parties should follow when conducting an investigation into potential employee misconduct regarding electronic communication tools. This is not intended to be a “how to” manual. Rather, this document is intended to highlight various factors that one needs to consider in identifying, obtaining, and preserving computer evidence. Each incident, or report of an incident, must be handled individually, in accord with the specific circumstances in the agency, including available resources, policy and agency culture.

The reader is strongly encouraged to consult with the appropriate Human Resource Professional and/or Department of Employee Relations Labor Relations Representative for further guidance and assistance in dealing with these issues. The issues that arise in employee misconduct of this nature frequently implicate a number of agency and/or Statewide policies and employment-related laws. The reader is also encouraged to consult with the appropriate Attorney General representative for further guidance and assistance in dealing with these issues.

II. Roles and Responsibilities

Agency management must have policies/guidelines in place for appropriate use of computer or Internet resources. The agency must further ensure that both new and current employees are aware of related policies, procedures, and work rules. If an employee does not have knowledge of computer and/or Internet specific policy(ies), it may be difficult to hold him/her accountable for the policy violations.

There should be a process for reporting an incident of computer or Internet misconduct. An investigation usually starts when an initial report/complaint is made; however; there are a number of different ways that an agency may become aware of this type of misconduct. A complaint could be made by anyone. In cases where the immediate supervisor is allegedly engaged in this type of misconduct, the policy and/or guidelines must allow for the report to go to someone else.

A. Incident Response Person

The role of the incident response person is to ensure that the information from the reporting individual is as complete as possible. The incident response person may be a supervisor, manager, or other person designated by the agency. If the incident response person is not someone from Human Resources, s/he must notify and coordinate with the agency Human Resources office after receiving the initial report.

B. Supervisor

The role of the supervisor in this process is extremely important, as the supervisor is typically in the best position to alert the agency to possible misconduct. Supervisors are responsible for assessing subordinates' use of electronic resources. A supervisor is also responsible for taking the appropriate action when s/he has reason to believe that employee misconduct has occurred. Supervisors must also strive to maintain a discrimination and harassment free work environment which is often jeopardized in cases involving this type of misconduct. Additionally, supervisors are responsible for keeping subordinates informed of policies, procedures and work rules.

C. Manager

The role of the manager in this process is to ensure that supervisors are aware of their responsibilities and that they are held accountable for those responsibilities. Managers are also responsible for keeping employees advised of policies, procedures and work rules and any changes or modifications that may be made. Additionally, managers are responsible for providing support and guidance to supervisors throughout the entire process.

D. Human Resource Professional

The role of the HR professional is to coordinate the investigation and to advise supervisors, managers, and other decision-makers of the proper investigation procedures and techniques. Please note that in some cases, the HR professional may conduct the investigation. The HR professional will also assist in the involvement of the IT manager, if such involvement is appropriate, and manager of the subject employee's division and will advise supervisors, managers, and other decision-makers of the consequences of taking or not taking action or pursuing an investigation.

The HR professional will also determine when to involve outside consultative contacts such as a technical services specialist, to assist with and coordinate the investigation. S/he will also contact the Department of Employee Relations Labor Relations Bureau and possibly the Attorney General's Office for information related to issues arising out of the labor agreements and/or the law.

E. Information Technology Professional

The role of the IT professional is to provide technical assistance and data recovery services to the agency HR professional or outside investigator. Preserving the integrity of the evidence is of critical importance in these investigations. The IT professional is key to maintaining the integrity of digital evidence and s/he must take great care with the computer evidence s/he is able to recover during the course of an investigation. That evidence is vital to the veracity of the investigation, and must be preserved for future purposes. If the agency utilizes monitoring or blocking software, it may be the role of the IT professional to administer and monitor those programs. Finally, it is the responsibility of IT professionals to report instances when they become aware of unusual or suspicious activity in the course of performing their normal duties. IT professionals need to have an understanding of their obligation to report suspicious activity, but to refrain from sharing private personnel data discovered or conducting investigations without prior authorization from an agency HR professional. Agencies also need to determine who will monitor the blocking or monitoring of the IT employees.

III. Incidents That Require Investigation

A. Impermissible Activities

Pursuant to the statewide policy regarding the appropriate use of electronic communication and technology, there are certain activities that are impermissible uses of State owned and operated computers and computer systems. When an agency has reason to believe such impermissible activities have occurred, it has an affirmative duty to investigate the allegations of misconduct. Such activities include, but are not limited to:

1. Illegal activities;
2. Wagering, betting, or selling ;
3. Harassment, disparagement of others, stalking, and/or illegal discrimination ;
4. Fund-raising for any purpose unless agency sanctioned;
5. Commercial activities, e.g., personal for-profit business activities;
6. Promotion of political or religious positions or activities;
7. Receipt, storage, display or transmission of material that is or may be reasonably regarded as violent, offensive, racist, sexist, obscene, sexually explicit, or pornographic, including any depiction, photograph, audio recording, or written word;
8. Downloading or installing software (including games and executable files) unless agency-sanctioned;
9. Unauthorized accessing of non-public data;
10. Non-State employee use (e.g. family member or friend) at work or at home;
11. Uses that are in any way disruptive, or harmful to the reputation or business of the State;
12. Purposes other than state business, except incidental or minimal use.

B. Reporting Sources

An agency may receive a report of misconduct from a number of different sources including, but not limited to:

1. Employee comments about self or others;
2. Accidental or intentional observation by co-workers;
3. Monitoring filters;
4. Technical staff observing something unusual; and
5. Complaints.

IV. Collecting Basic Information

The investigation itself is the responsibility of the agency HR professional or other designated professional and the gathering of evidence must be done under the direction and control of that authority.

A. Getting Started

When beginning an employee misconduct investigation, there is certain basic information that the agency will want to obtain at the onset. This basic information includes, but is not limited to:

1. Nature of the incident(s);
2. Name, phone, and work location of every person involved (person who made initial report, employee (s), supervisor, witnesses, etc.);
3. Date, time and locations of incident(s);
4. Single incident or known pattern;
5. Technical expertise level of the employee(s) involved;
6. Other persons who may know that a report was made;
7. Type of equipment involved;
8. Type of application:
 - a. E-mail;
 - b. Browser;
 - c. Picture viewer;
 - d. Power point;
 - e. Print materials; and/or
 - f. Other.
9. Whether the employee knows that s/he was observed (destruction of evidence issue); and
10. Name of technical contact for the employee's area.

B. Involving Law Enforcement Officials

Under rare circumstances, the HR professional will need to contact outside law enforcement authorities. Such action is very serious, and should not be taken lightly or without the consultation of management when practicable. Supervisors and managers should refrain from taking such action until they have had an opportunity to consult with the agency HR professional. The rare circumstances under which such action may be necessary include, but are not limited to:

1. If the investigation involves “imminent harm”. Imminent harm means delay could result in serious injury or death. In this situation, the HR professional should contact **Local Law Enforcement or call 9-1-1 immediately**.
2. If the investigation involves sexual activity/images with persons who appear to be under the age of 18, immediately contact **Local Law Enforcement**. Local Law Enforcement Officials will make the determination as to when and if the Internet Crimes Against Children Task Force should be contacted for additional assistance. *Note: For additional information, see MINN .STAT. §617.246.*
3. If the investigation involves embezzlement, extortion or unlawful use of public funds or property, check with the agency auditor and contact the Legislative Auditor, as required in MINN. Stat. §609.456, subd. 2 (see the Resources section, page 18).
4. If the investigation involves violation of the law, contact the Employment Law division of the Attorney General’s office.

Please note that Chapter 352 of the 2002 Session Laws authorizes HR professionals to call law enforcement and share private personnel data about possible crimes.

V. Determining the Scope of the Investigation

After the basic information is collected it will be necessary to make some preliminary decisions regarding the scope of the investigation. For example, the agency may decide that it will investigate persons who received and then forwarded inappropriate images, but not persons who only received and then deleted these images. Or, the agency may want to limit the investigation to activities that occurred within a specific time frame, e.g. the last six months. Finally, the agency may also find it necessary to notify other agencies if employees are e-mailing inappropriate messages across agencies. In some cases, the agency may not be able to determine the scope of the investigation until after the collection of some initial evidence.

Once the agency determines the scope of the investigation, the agency will need to identify individuals who will work on the investigation. Clearly, the agency will want to involve a HR and IT professional, but in addition, the agency may want to consider including the subject employee’s supervisor and/or manager. Additionally, if the

investigation is unusually large, the agency may want to assign multiple investigators, designating one as lead investigator and other individuals to conduct interviews. Finally, the agency will want to make a decision on whether to use an internal or external investigator/lead investigator. In making this decision, the agency should consider:

- a. The ability of investigator(s) to maintain objectivity;
- b. The fairness, or perception of fairness, of the investigation if internal investigators are used;
- c. The possibility of further legal or criminal penalties;
- d. The level of difficulty of the case; and
- e. The experience of the investigator.

VI. Obtaining Computer Evidence

Think carefully about how and where to secure evidence and work with all investigation participants to create documentation of all steps taken and decisions made during the process.

Agency staff will want to keep the number of people who are aware of the complaint and subsequent investigation as limited as possible. Keep in mind that the allegations made against the employee are allegations that have been neither substantiated nor unsubstantiated. In the event that the allegations are substantiated, the labor agreements require disciplinary actions to be private, and agencies need to be respectful of this. Please note that once final disposition of the discipline occurs, pursuant to MINN. STAT. §13.43, that data become public.

A. The Subject Employee

HR professionals should carefully select one of the options discussed in Section VII below and then coordinate the agency response accordingly. For example, the HR professional may need to coordinate the removal of the employee from the environment so that the IT or HR professional can collect evidence including the computer hard drive, or the agency may wait until the end of the workday to collect the evidence. Placing the employee on paid investigatory leave while the investigation is pending may also be necessary. The HR professional should refer to the appropriate labor agreement for information regarding the placement of employees on investigatory leave. If this step is necessary, it is advisable to seize the employee's computer before s/he is notified of the leave. Make sure to cancel all employee passwords so that the employee cannot go into the system and destroy evidence.

B. Surveying the Workstation

If the investigation involves more than just e-mail, and the IT or HR professional has the opportunity, the collection of computer evidence should start before anything is touched or moved in the employee work area by taking photographs of the employees' workstation. Take note of the computer, all peripherals, plug in

connections, “post it” notes, positioning of monitor in workspace, articles hindering view of monitor screen such as screen guards, rear view mirrors mounted on monitors, or other such items.

In addition to physical alterations to the workstation, there are other very valuable sources of information in close proximity to the employee’s computer. For example, consider surveying:

1. “Post It” notes;
2. Calendars;
3. Folders marked “funnies” or “personal”;
4. Floppy discs;
5. CD ROM’s;
6. Trash baskets; and
7. Recycle baskets.

Agencies should be cautioned that there are special considerations when it comes to searching certain types of property within the employees’ office or cubicle.

1. Personal Property

As a general rule, searching lockers locked with personal locks, personal items such as purses or wallets, personal vehicles, or a non-agency owned personal e-mail accounts (i.e. Hot Mail, Yahoo, AOL) as part of an employee misconduct investigation is not advisable and agencies are cautioned to consult with the Labor Relations Bureau prior to engaging in such activity. The agency may be able to obtain access to these areas by asking the employee for permission.

2. State Property

Agencies must take care to notify all employees, either via written memo or policy, that the agency retains the right to search any and all State owned property, including but not limited to, locked desk drawers, locked file cabinets, and locked State vehicles. Providing employees with advance notice that State property can be searched at any time will lower their expectations of privacy. Failure to alert employees that the agency retains this right may limit the agency's ability to search locked areas, even though it is State property.

Please note that some agencies, such as the Department of Corrections, have statutory authority allowing access to locked drawers and personal items at the facilities.

Similarly, do not open e-mail the employee has not yet opened. This issue is still unsettled in the courts. If it is determined that it is critical to go into unopened e-mail to conduct the investigation, first check for guidance from your agency legal advisors.

After the IT or HR professional has completed these tasks, s/he should seize the computer hard drive.

C. Handling the Hard Drive

Once the IT or HR professional has seized the hard drive, and it is time to collect the actual computer data, s/he must not allow someone to simply “check out” the potential computer evidence. The importance of having a properly trained computer evidence specialist process the computer evidence cannot be overstated. Computer evidence is very fragile. Such evidence can easily and unintentionally be altered or destroyed. Simply booting the computer and/or running Microsoft Windows can overwrite vital computer evidence. Additionally, timelines of computer usage and file accesses are valuable sources of computer evidence. The times and dates when files were created, last accessed, and/or modified can make or break a case. Opening a file will change the last access date and potentially damage a case. The HR or IT professional must carefully document the dates/times that access to the employee’s account took place. Documentation should be made of the dates/times the investigator had access to compare with the times the employee had access, in the event that there is any question as to the veracity of the evidence.

The IT or HR professional will also want to determine how to recover and protect the data so that the employee is not able to alter or destroy it. A technically savvy employee may have the computer configured so the computer will destroy evidence automatically. The agency must be able to demonstrate that evidence has not been altered or compromised.

The HR professional also needs to be aware that dependent upon the nature of the computer misconduct, IT professionals, supervisors, and managers may have an extremely difficult time viewing the images that are collected as a result of these investigations. If this type of issue presents, the HR professional is strongly encouraged to contact the Employee Assistance Program for assistance in dealing with this issue at the onset of the investigation.

D. Other Sources of Evidence

In addition to surveying the subject employees’ workstation and seizing the computer hard drive, the HR or IT professional may also want to consider exploring the following alternative sources of evidence which include, but are not limited to:

1. Unlocked or locked desk drawers and file cabinets;
2. Fax area;
3. Printer area;
4. Firewall logs;
5. Review of e-mail – messages sent, received, in the trash, and those saved in folders;
6. Copies of network storage areas;
7. State owned Personal Digital Assistants or PDAs (e.g. Palm Pilots);

8. State owned cell phones;
9. Cell phone billings; and
10. Digital cameras.

Agency personnel must be very thorough in collecting all sources of evidence. There may be situations, however, when the agency decides that there is sufficient evidence and ends the investigation. There may also be instances where the evidence does not substantiate the allegations, and the agency would then simply close the investigation and return any employees who are on paid investigatory leave back to the workplace.

Important Reminder: Always consider “chain of evidence” issues – document who has the evidence, secure the storage area, etc.

VII. Timing the Collection of Computer Evidence

There are a number of factors to consider in timing the collection of computer or Internet evidence. For example:

1. Can the IT or HR professional obtain the evidence without alerting co-workers?
2. Is the employee aware of the report/observation? Is evidence likely to be destroyed?
3. Is another person being harassed?
4. What is the location of the computer/lap top? Is it on- or off-site?
5. Does the agency have the capability of monitoring?
6. Does time permit a plan for monitoring?
7. Will monitoring be likely to yield additional evidence?
8. Any risk of exposing others to inappropriate materials if the agency does not act immediately?
9. What is the risk of publicity with each option?
10. What is the risk of a defamation claim by the employee?
11. Are other employees in the work group already aware of the situation?

When collecting computer evidence, the IT or HR professional needs to make some critical initial decisions on when to collect the relevant evidence. Generally, there are three basic options available to the IT or HR professional:

A. Seize the Computer Hardware/Software NOW – Option 1

If the nature of the allegations makes it necessary to immediately seize the potential evidence, the agency must make a number of critical decisions in a very short period of time. For example, the agency will want to consider:

1. Who will do it? (human resources, technical support individual, supervisor, manager, or lead investigator)
2. Will the person responsible for seizing the data perform a sequenced shut down or cut all power at once? (Keep in mind that cutting power at once is drastic and the loss of evidence or damage to the operating system could occur. It may, however,

be necessary if the computer is configured to destroy evidence if a sequenced shut down is used.).

3. Will other employees observe the process?
4. Is this necessary to prevent the employee from taking evasive measures from a remote location?
5. Is it necessary to restrict the employee's access to the building/work unit area?
6. Can the network administrator suspend access rights immediately?
7. Will a ruse of some sort be necessary? For example:
 - a. "We're going to upgrade your computer."
 - b. "Can you bring in your state owned computer for an upgrade?"

Note: Obtaining evidence NOW is rare. Consider using this approach only in the most extreme circumstances where immediate action is necessary.

B. Obtain the Evidence LATER When Employee Is Not Present – Option 2

This is the most common method for an agency to utilize. In selecting this option, the agency will have additional time to consider the following:

1. Determine the necessary preparation to ghost the hard drive (see page 14).
2. Determine who needs to be involved.
3. Determine when the evidence should be seized – before or after work hours or perhaps on the weekends or the employees' day off?
4. What are the risks associated with waiting?
 - a. Is data likely to be lost or over written?
 - b. Does the incident appear to be isolated or repeated behavior?
 - c. Is the employee suspicious?
 - d. Is the employee technically savvy?

C. Monitor and Obtain Evidence at a Later Date – Option 3

The agency must decide IF they will monitor, WHO will monitor, and HOW monitoring will be accomplished. If the agency decides to monitor, or decides to do a combination of monitoring and then obtaining evidence, it will need to select the items to be monitored. For example:

1. Firewall logs/network logs – times in, times out;
2. E-mail (Set aside back up tapes so they are not inadvertently recycled);
3. Make periodic "ghost" images – to monitor on line "chat room" activity; and
4. Tracking the employee's whereabouts and usage:
 - a. Work product;
 - b. Phone activity;
 - c. Parking lot cards;
 - d. Use of ID/security/proximity cards; and
 - e. Time sheet records.

Note: The IT or HR professional may need to modify regular technical support procedures performed by information technology staff so that data is not erased/modified during the monitoring period.

VIII. Preserving Evidence (Chain of Custody)

As is true with all investigations, it is critically important that the IT and/or HR professional involved in collecting evidence carefully document collected evidence – including all steps in the collection process. The IT professional who obtains the evidence must be able to articulate these steps if there is a subsequent arbitration or other administrative or judicial hearing. Specifically, the agency will want to document the following:

1. From whom or where was the evidence obtained?
2. Who has custody of the evidence?
3. How was the evidence stored – secure or locked area?
4. Will the storage area prevent environmental degradation (for example magnetic fields, heat, moisture, and/or dust)?
5. Identify each piece of evidence as specifically as possible:
 - a. Description of the item (labeling);
 - b. Asset or serial number;
 - c. File size, date, origin;
 - d. Owner; and
 - e. Case name.

Again, please note that the employee is entitled to access to and/or a copy of the data to the extent necessary to utilize their rights under due process and the collective bargaining agreement. Additionally, pursuant to MINN. STAT. §13.43, the data are public after final disposition of the discipline.

Note: Electronic evidence must be migrated to a permanent, non-modifiable media. The IT professional will need specific tools for this. The IT professional may want to make two copies, and conduct reviews from the copy of the copy. With network storage drives, copy it out to another drive with limited access (maybe only the investigator and technical administrator). The agency will need to retain this evidence at least until the investigation is closed, all discipline (if any) has been applied, and all grievance hearings, arbitration hearings and litigation are concluded. Please note that this process could take several years. After that, the evidence should be handled according to agency record retention schedules.

IX. Technical Aspects of Hard Drive Evidence

To obtain an original hard drive without employee knowledge, the IT professional will need to make a “ghost image” or exact copy of the hard drive. Creating a ghost image of the subject employee’s hard drive provides a number of benefits to the agency. For example:

1. The employee should not be able to detect any alteration or modification to his/her computer.
2. This gives the agency additional time to assess the situation and to take appropriate measures.
3. Clients, co-workers, and others will not be aware that an investigation into the subject employee's computer activities is occurring, which will allow the agency to preserve the employee's reputation.
4. This preserves availability of vital business processes that may be in the computer.

If the IT or HR professional elects to make a ghost image of the subject employee's hard drive as part of the investigation process, there are certain basic steps that must be followed. Those basic steps are as follows*:

1. Seize the employee's hard drive.
2. Use specially designed utility to get employee's system date and time.
3. Boot employee's computer off a customized boot floppy with Norton ghost on it.
4. Run Norton Ghost from floppy using the multicasting feature.
5. Use network connection to ghost hard drive.
6. Drop ghosted image to new hard drive.
7. Swap the new hard drive with the employee's original hard drive.
8. Boot employee's system with the new hard drive in it.
9. Reboot employee's machine to verify it boots normally to the network login prompt.
10. Put everything back (notes, calendars, pens, etc) EXACTLY where they originally were.

**Please note that this is not a comprehensive "how to" and the actual steps may vary.*

Note: Get help if the IT or HR professional needs advice on this or other hard drive processes. (See RESOURCES Section, page 10).

X. The Investigative Interview Process

Once the collection of data is completed, the HR professional or designated investigator will want to begin conducting interviews with the subject employee(s) and any and all individuals who may have knowledge or information regarding the specific allegations. If the behavior involves sexual harassment, follow the procedures outlined in the Affirmative Action Plan, Sexual Harassment policies and bargaining contracts. Check with the agency HR office for these procedures.

The HR professional will want to be conscious of the rights of the subject employee(s) throughout the interview process. The various labor agreements contain very specific rights for employee interviews that may result in discipline for the interviewed employee. If the HR professional has any questions as to what those rights are, how to ensure those rights are protected, or who and when an employee is entitled to these rights, s/he should contact the Department of Employee Relations Labor Relations Bureau for guidance before starting the interview process.

The HR or other professional who will be conducting the interviews will also want to carefully and thoroughly review any and all technical data collected and relevant policies or rules before conducting interviews. If the employee is not currently on investigatory leave the HR or other professional will want to determine if such a measure is necessary at this juncture in the process.

A. Interview Process

1. Union Representation

At the onset of the interview, the HR or other professional will need to provide every represented employee who could be disciplined as a result of the interview with Union Representation. If the employee declines Union Representation, be sure to have the employee sign a waiver of representation form. If the represented employee is simply being interviewed for information gathering purposes, and the agency does not reasonably expect that it will discipline this employee, then the employee does not have a contractual or legal right to representation unless provided for in the applicable bargaining agreement (i.e. sexual harassment complaints).

2. Tennesen Warnings

The HR or other professional will also need to provide suspected employees and witnesses with a data practices notice (Tennesen warning) While every HR office should have a form developed for this purpose, DOER Labor Relations can provide recommended formats. A Tennesen warning advises employees of the purpose and intended use of the requested information, whether the employee may refuse or is required to provide information, consequences for providing or refusing to provide information, and who will have access to the information (see Minnesota Government Data Practices Act, MINN. Stat. §13.04, Subd. 2). Be prepared to respond to questions about data privacy.

3. Garrity Warnings

Agencies should exercise extreme caution in providing an employee with a Garrity Warning, particularly in investigations involving potentially illegal activities. Once an agency gives an employee a Garrity Warning, the receiving person cannot be criminally prosecuted for the information they disclose. Accordingly, it is of critical importance that the agency consults DOER Labor Relations to determine if this is an appropriate option.

B. Develop Questions

As previously stated, the HR or other professional who is conducting the interviews must review any and all evidence and complaints while developing questions to ask.

The interviewer must be skilled enough that s/he can immediately ask relevant follow up questions that had not been anticipated during the preparation.

The questions should stick to the facts of the case and/or allegations. The interviewer should maintain control over the interview and not allow the questions to get off track. The interviewer also needs to be aware that if a Union Representative is present, the Union Representative's role is to assist the employee and ensure the employee's rights are not violated. The Union Representative is not there to advocate for the employee, or engage in any adversarial or confrontational exchanges with the interviewer.

C. Determine the order of the interview(s)

The HR or other professional should first interview the complainant, if there is one, to hear the details of the complaint/issue. Ask the person who else they think may have pertinent information and should be interviewed. The next group to be interviewed is the witnesses. The HR or other professional should take care to interview only those employees who have direct knowledge of the situation and not those who may only be able to offer hearsay evidence. The final interview should be the subject employee. Keep in mind that after interviewing the subject employee there may be a need to recall or re-interview certain witnesses for clarification purposes. Make sure to reserve the right to call the person back into subsequent interviews.

D. Conducting the Interviews

The HR or other professional may develop letters to be sent to witnesses and the subject employee notifying them of the need for the interview, the date, time, and location of the interview, and finally, whether the employee has the right to Union Representation at the interview. Be sure to confirm with the interviewee in advance of the interview.

When the time comes to actually conduct the interviews, the HR or other professional will want to determine where and when to conduct the interviews. The HR or other professional should consider conducting interviews outside of the work area so that employees and witnesses have privacy. This will also provide a neutral setting, and if allegations of sexual harassment are involved, keep the complainant and respondent separate. In general, interviews should be strategically scheduled so those individuals are not running into each other on the way in or out of the interview. If the interview could result in criminal charges, coordinate the interview with local law enforcement officials.

Finally, the HR or other professional will need to determine whether to use tape recorders. Some interviewers and agencies routinely tape record all employee investigatory meetings to be later transcribed. Keep in mind the agency's past practice and the appropriateness of this for the specific situation at hand. For example, if this is a large investigation, involving a number of interviews, this may be the best way to keep all of the information organized. Please note that neither the

employee being interviewed, nor the Union Representative should be allowed to record the interview. In order to protect the integrity of the investigation, DOER Labor Relations recommends that taped interviews and transcripts of tapes not be released to the subject of the interview while the investigation is still active. Once the investigation is complete, and discipline has been administered, the agency may release such information. One exception to this is that the complainant has a legal right to the tape or transcribed copy of the statement that he/she provides during the course of the investigation (see Minn. Stat. §13.39, Subd. 2. (b)).

XI. The Discipline Process

Before reaching the decision making phase, agencies must take care to ensure that they have appropriately investigated the alleged acts of misconduct and gathered supporting documentation. For additional information on conducting an investigation on computer misuse/abuse, the reader should refer to the Investigation section.

Once the appropriate agency personnel have completed the investigation and subsequent investigatory report, the Human Resource professional should work with the agency personnel who are charged with making the final disciplinary decision in the pending matter. Agency staff should take care to avoid a lengthy decision making process and ensure that any disciplinary decisions are made within a short period of time following the completion of the investigatory report.

When making the disciplinary decision, agency personnel must carefully consider and weigh a number of different factors in determining the appropriate level of discipline. For example, agency personnel will need to determine if there is any evidence of illegal activity. If so, the individual making the decision may be needed to testify as a witness in any subsequent legal action or arbitration. In addition to possible legal implications, the decision-maker must also be aware of the other possible policies that may be implicated in a given situation. For example, if an employee is viewing sexually explicit websites, an agency's sexual harassment policy may be implicated. Or, if the individual is looking at violent, sexually explicit websites, an agency's violence in the workplace policy may be implicated as well. The decision-maker should remain cognizant of the various policies that may be at issue and not limit the possibilities to just the computer or Internet specific policies. If numerous policies are implicated it may be grounds for a higher level of discipline.

In addition to multiple policy violations, the agency will want to consider a number of factors that may cause the level of discipline to be more or less severe. These considerations include, but are not limited to the following:

1. How long has the employee been employed by the state?
2. Does the employee have any previous incidents of discipline?
3. What is the impact of the type of misconduct on the agency's reputation?
4. How much State time did the employee spend engaged in these activities?

5. If this is a large investigation involving a number of employees, what was this employee's level of involvement? Did s/he search out and send inappropriate information or was this employee only on the receiving end?
6. Did the employee's work product and/or production decrease?
7. Are there legal implications surrounding the misconduct? For example:
 - a. Hate based Internet sites or e-mails?
 - b. Sexually explicit Internet sites or e-mails?
 - c. Sexually explicit images involving minors?

Reviewing all investigation documents is a very important part of making a disciplinary decision. The individuals making the discipline decisions must review the images, data, or other documentation of misconduct so that s/he understand the nature of misconduct involved. The decision-maker will be in a better position to make factually based disciplinary decisions if all of the relevant documentation is reviewed. It may also be necessary to meet with the investigator to clear up any questions the decision-maker may have. While it would not be appropriate to solicit the investigator's opinion on what level of discipline is warranted, it may be helpful to solicit his/her opinion on how the case at hand compares to other cases the investigator has been involved with. The decision-maker may find it helpful to know if this case has a relatively high or low number of inappropriate activities or how the amount of time the subject employee spent engaged in the misconduct compares to other cases.

Finally, but certainly not least, the decision-maker should also consult with the HR professional for a comparison with other internal agency cases. This will help to ensure that the agency remains internally consistent. Either the decision-maker or the HR professional should also contact DOER Labor Relations for further consultation to ensure that the agency does not take an action that would be inconsistent with the statewide standards. The DOER Labor Relations staff will also be able to provide information on similar cases to help guide the agency in making its own decision.

When an agency believes that the employee misconduct may be subject to criminal prosecution, the agency should contact their Labor Relations and Attorney General representatives prior to interviewing the employee. The agency, the Labor Relations Bureau, and the Attorney General's Office will need to give careful consideration to coordinating the agency's needs in pursuing the internal employee misconduct investigation with the local prosecutors interest in pursuing a criminal investigation and prosecution. There are also competing evidentiary issues associated with the two investigations that must be carefully balanced and coordinated. Failure to coordinate the potential criminal matters with the internal misconduct investigation can result in serious evidentiary issues and extraordinarily long delays in the internal decision making process with ongoing pay or backpay concerns.

XII. Post Investigation Activities

Activities subsequent to an investigation can be as important, if not more important, than the investigation itself. The nature of such investigations can be emotionally and

mentally draining on those challenged to be objective yet thorough investigators and interviewers.

In light of the toll such investigations can take on those involved, the following activities are offered as suggestions to deal with the after effects:

1. Coordinate debriefings for affected employees with an Employee Assistance Program (EAP) provider. The agency may want to consider separate debriefings for witnesses, investigators, union stewards, management, etc.
2. Ensure all documentation is in order and maintained in a secure place so that those who are not authorized to have access under the Data Practices Act cannot access it.
3. If the agency needs to put a computer back into production, be sure that all inappropriate text/images have been removed from the hard drive. This is to ensure that all traces of this material are eliminated before another employee uses the workstation.

XIII. Conclusion

This guide is intended as a resource for State of Minnesota employees who may be involved in the initiation, implementation, or evaluation of an investigation involving evidence found on computers or computer systems. While no guide can address every issue or concern that may arise, this guide is designed to help with the investigation process. Always contact the agency Human Resources office; they are the main resource. Other important resources to consider include DOER Labor Relations, or other resources cited below. Many agencies have experience in one or more aspects of computer related employee misconduct and investigation and can be very helpful in sharing “lessons learned.”

XIV. Resources

1. **Attorney General’s Office – Employment Law Division:** 651-2825729
2. **DOER--Employee Assistance Program:** Kimberly Peck, Manager, 651-296-9722
3. **DOER--Labor Relations:** 651-296-2516
4. **Legislative Auditor:** Jim Nobles, 651-296-4710
5. **Technical Resource:** Gary L. Johnson, Department of Human Services, CPA, CISA, Computer Audit Specialist, 651-215-1810

Additional References:

“Computer and Internet Usage – Blocking and Monitoring Guidelines”
“Statewide Policy: Appropriate Use of Electronic Communication and Technology”
Administrative Procedure 1.2 – Harassment Prohibited
Statewide Policy – Zero Tolerance for Sexual Harassment
MINN. STAT. §1.50 – Freedom From Violence
MINN. STAT. §15.86 – State Agency Actions.