HR/LR Policy #1429 Data Protection Policy for Human Resource Systems	**Issued** **Revised** **Authority**	12/01/2014 Enterprise Human Resources

OVERVIEW	
Objective	To ensure that not public data contained in Human Resource Systems are accessible only to persons within the State agency whose work assignment and job duties reasonably require access to the data.
Policy Statement	State agencies and employees who are entrusted with access to not public data contained in Human Resource Systems must take measures to ensure that the security of the data is protected.
Scope	This policy applies to employees of executive branch agencies and employees in the Office of Legislative Auditor, Minnesota State Retirement System, Public Employee Retirement system and Teachers' Retirement System, who are provided access to any Human Resource System in the course of their job duties.
Definitions	**Government data.** All data collected, created, received, maintained or disseminated by any State agency regardless of its physical form, storage media or conditions of use. **Human Resource Systems**. Include but are not limited to, HR Solutions, ELM, MNSight, Resumix, Recruiting Solutions, agency-based Human Resource systems and databases, computer hard drive, computer desktop, personnel files, medical files, and any other means of accessing private personnel data. This includes all private personnel data, whether in paper or electronic form. Human Resource Systems do not include an employee's own Self-Service account. **Human Resource Classification.** For purposes of this policy, "Human Resource Classification" includes all individuals who are provided access to any Human Resource System in the course of their job duties or for purposes of a work assignment which reasonably requires access to a Human Resource System, regardless of whether the individual's normal job classification is in the Human Resources job series. **Medical data**. Personnel data regarding the medical condition or history of an employee. **Not public data**. Government data that is classified by state or federal law or temporary classification as not accessible to the public. Some not public data is also not accessible to the subject of the data. See Data Practices For Personnel Records and M.S. 13.02. **Personnel data**. Any government data on individuals maintained because the individual: (a) is or was an employee of a State agency; (b) is or was an applicant for employment by a State agency; (c) performs services on a voluntary basis for a State agency; or (d) acts as an independent contractor with a State agency.

OVERVIEW	
	State agency. The particular State department, commission, board, or institution, or other employing entity for the employee governed by this Policy.
Exclusions	N/A
Statutory References	M.S. Chapter 13, Minnesota Government Data Practices Act: www.revisor.mn.gov/statutes/?id=13

POLICY REQUIREMENTS

I. STATE EMPLOYEE ACCESS TO NOT PUBLIC DATA

A State agency employee may access, acquire, view or use not public data contained in Human Resource Systems only when the employee is reasonably required to do so in order to accomplish a work assignment or to satisfy the employee's job duties on behalf of a State agency. Access to this data is limited to business purposes only, and must not be used for personal use or inquiry. In the event of a temporary duty as assigned by a manager or supervisor, an employee may access not public data needed to complete the assignment for as long as the work is assigned to the employee, but no longer than the assignment requires.

Employees may be subject to disciplinary action, up to and including discharge, if the employee accesses, acquires or views not public data:

- when the employee is not reasonably required to do so in order to accomplish a work assignment or to satisfy job duties on behalf of a State agency;
- for purposes other than to accomplish a work assignment or to satisfy job duties on behalf of a State agency.

Knowingly obtaining, accessing, or viewing not public data without being reasonably required to do so in order to satisfy the employee's work assignment and/or job duties, without the informed consent of the individuals who are the subjects of the data, or without statutory authority, and with the intent to use the data for nongovernmental purposes, constitutes a misdemeanor under Minn. Stat. § 13.09(a).

Any employee who discovers that another employee has accessed, obtained or viewed not public data when not reasonably required to do so in order to accomplish a work assignment or to satisfy job duties on behalf of a State agency, or for purposes other than to accomplish a work assignment or to satisfy job duties on behalf of a State agency, shall promptly notify the State agency's Human Resource Director, Assistant Commissioner, Deputy Commissioner or Commissioner.

State employees who are entrusted with access to not public data have a duty to protect the data from unlawful disclosure and to act in such a way as to reduce the threat of a breach in the security of not public data by others.

It is the responsibility of each employee to comply with this policy and the standards and procedures identified in this policy. It is the responsibility of all managers to implement and enforce compliance with this policy. Each State agency will enforce compliance with this policy. Suspected breach of this policy will be subject to investigation. Any employee who is determined to have breached this policy may be subject to disciplinary action, up to and including discharge.

II. STATE EMPLOYEE ACCESS TO HUMAN RESOURCE SYSTEMS

In order to protect the security of not public data, State agencies and employees given access to not public data in Human Resource Systems must comply with the following requirements. The following list is not exhaustive. Exercise common sense and due caution with all not public data. Data protection is every

POLICY REQUIREMENTS

employee's responsibility.

1. Access. Employees shall be given access only to those particular Human Resource Systems to which access is reasonably required in order to accomplish a work assignment or to satisfy the employee's job duties. Employees of one State agency shall not be given access to not public data of another State agency unless the access is authorized by law or the agency receives the informed consent of the subject of the data.

2. Minimum Necessary Use. Employees must view, use and release not public data only to the extent that is necessary to do their jobs. For example, employees must:

    - Discuss or otherwise release not public data only as needed to do the employee's job.
    - Limit access and review of not public data to information required to do the employee's job.
    - When doing database searches in databases containing not public data, use search words that limit results to what the employee is looking for.

Employees must not:

- Search for or access not public data on any matter not assigned.
- Look up information about family members, ex-family members, friends, neighbors, acquaintances, celebrities, the employee's own self, or anyone else whose data is not necessary to do the employee's job.
- Use database screens containing not public data for training purposes.

3. Passwords. Employees who are given access to electronic Human Resource Systems are prohibited from sharing their access passwords. Passwords must be secured and must not be stored or posted in any accessible location.

4. Workspaces. Employees who have not public data on desktops or visible on their computer monitors must take precautions to ensure that visitors to their workspace cannot view not public data to which the visitor does not legitimately have access, including by locking the computer during the visit. Employees must log off of any electronic Human Resource Systems or lock their computers when their workspace is unattended.

5. Email data. Employees must not send not public data via the Internet or unsecured networks unless the information is encrypted. Encrypted or "secure" messaging allows email users to protect not public data when it is emailed or sent as an attachment to an email. Employees are required to encrypt all messages that contain not public data when sending this type of data outside of the IT Consolidated Agencies (see list below). Encryption is enabled by typing [encrypt], [secure], or [encrypted] anywhere in the subject line. **NOTE:** Email messages between IT Consolidated Agencies' email users are automatically encrypted in transit so no additional steps are necessary.

    Employees must ensure that the email contains the correct addressee; encrypted data sent to the wrong person will still be accessible by that person. Employees must also ensure that the subject of the data has given written informed consent for the data to be transmitted to the addressee, or the addressee has statutory authority to receive the data.

    The electronic transmission should include a statement concerning the private nature of the information being sent and a warning not to release the information inappropriately, and to notify the sender if the information was received in error.

    Employees should not request individuals to provide social security numbers or other not public data to

the State by email unless the data is encrypted.

6. Facsimile. Sending and receiving not public data by facsimile is discouraged. Whenever possible, not public data should not be sent by facsimile, and instead sent by encrypted email. If facsimile transmission is necessary, the sender must take steps to ensure that the data is being sent to the correct facsimile number and should notify the recipient that a facsimile is about to be sent. The sender should also confirm receipt by the intended recipient. The facsimile should include a statement concerning the private nature of the information being sent and a warning not to release the information inappropriately, and to notify the sender if the information was received in error.

7. Shared Spaces. Copies of documents containing not public data must be immediately removed from copiers, printers and facsimile machines that are not located in private offices. Browsing of documents left at copiers, printers and facsimile machines, other than to determine the owner of the document, is prohibited.

   When necessary to discuss not public data, conversations should be conducted in a manner so as to safeguard the data; for example, to the extent feasible, in closed offices or behind partitions.

8. Removing Not Public Data from State Property or Systems. Employees may only remove not public data from State property or systems if they have a work-related purpose to do so, and must have prior approval from their supervisor or manager. This includes both paper and electronic not public data. It also includes copying or forwarding not public data in order to transport or access the data off site or by means of a non-State email account or non-State computing device. A single approval may be granted by the supervisor or manager to cover repeated or similar needs to remove not public data. Employees removing not public data from State property or systems must ensure that the data, information or electronic equipment containing the data is secure and protected from theft or loss. Employees must ensure than any computing devices or electronic or paper media containing not public data in their possession or realm of responsibility is stored and transported in a secure manner. Employees must ensure that any not public data removed from State property or systems is not accessed by or accessible to anyone other than an agency employee whose job responsibilities reasonably require access, and must ensure that the data is either returned to the workplace, or is disposed of as provided below.

9. Disposal. All not public data shall be retained and disposed of as required by the State agency's document retention policy. When not public data is disposed of, it must be shredded, erased or otherwise destroyed in such a way that prevents its contents from being determined, and makes the not public data inaccessible, unreadable, unrecoverable and not capable of being reconstructed.

10. Medical Data. Medical data must be collected and maintained on separate forms and in separate physical or electronic files from non-medical personnel files and records. Medical data must be stored so that access is limited to only individuals in Human Resource Classifications whose job responsibilities require access. For physical medical files, this means that the files must be stored in a locked cabinet or office when not in use or unattended. Managers and supervisors must not be given access to the medical data of their staff members, except that supervisors and managers may be informed regarding necessary restrictions on the work or duties of the employee and necessary accommodations, and first aid safety personnel may be informed, when appropriate, if the medical condition might require emergency treatment.

11. Conflicts of Interest. When an employee has a work assignment requiring access to not public data about an individual who that employee has a relationship with, such that the employee's access to the data would constitute a conflict of interest or potential or perceived conflict of interest, the employee should immediately advise the employee's supervisor. The supervisor may transfer the work

assignment to another employee.

12. Protocol for Requests by Data Subjects. Agencies must develop a protocol for when a data subject seeks to gain access to private data about himself or herself contained in Human Resource Systems. The agency will take reasonable measures to ensure that the individual making the assertion is in fact the subject of the data. These measures will include that the individual must appear in person at the offices of the State agency to gain access and provide reasonable identification. In the alternative, if the individual does not make a personal appearance, the individual must provide the agency with a signed statement requesting the data and asserting that the individual is the data subject, and provide reasonable identification. If an individual asserts that he or she is the authorized representative of the data subject, the individual must provide reasonable identification, and present a consent form signed by the data subject, specifying the data to be released, and authorizing the release of the data to the authorized representative.

Every employee who is provided access to any Human Resource System in the course of his or her job duties or work assignments must be given a copy of this Policy and must sign the Acknowledgement below (provided under "Forms"). The signed Acknowledgement must be kept in the employee's personnel file.

III. TERMINATING ACCESS TO HUMAN RESOURCE SYSTEMS

An employee's access to Human Resource Systems must be inactivated immediately if the employee:

- separates from service with the State agency;
- moves to another position in the State agency that is not in a Human Resource Classification;
- no longer has job duties or a work assignment that requires access to a particular Human Resource System;
- is on a leave of absence; or
- is placed on investigatory leave.

The State agency must promptly notify MN.IT @ [the State agency], or MN.IT Central if there is no MN.IT staff at the agency, in order to terminate the employee's access to electronic Human Resource Systems.

Employees are prohibited from removing, taking, copying, emailing or downloading any not public data from Human Resource Systems when the employee:

- leaves service with the employing State agency;
- experiences a job change to a non-Human Resource Classification for the State agency; or,
- no longer has job duties or a work assignment for the State agency that requires access to the not public data.

Templates. An employee employed in a Human Resource Classification by a State agency, who voluntarily leaves service with the State agency for an appointment in a Human Resource Classification with another State agency or with a political subdivision of Minnesota, may copy, email or download templates for use in other government work. However, templates must not contain any not public data, and the employee must obtain prior supervisor permission and review prior to copying, emailing or downloading templates for use in other government work.

An employee who is discharged or non-certified from service in a Human Resources Classification, an employee leaving service in a Human Resource Classification for an appointment not in a Human Resource Classification, or an employee leaving service in a Human Resource Classification for an appointment with a non-government entity, may not take any data or templates from Human Resource Systems, regardless of the classification of the data. Such an employee may make a request for data pursuant to the provisions of the Minnesota Government Data Practices Act, Minn. Stat. §§ 13.03, subd. 1 ("Access to Government Data, public

POLICY REQUIREMENTS

data"); 13.04, subd. 3 ("Rights of Subjects of Data, access to data by individual").

LIST OF IT CONSOLIDATED AGENCIES (emails between these agencies are automatically encrypted):

Board of Psychology
Board of Pharmacy
Board of Veterinary Medicine
Board of Cosmetologist Examiners
Board of Marriage & Family Therapy
Board of Behavioral Health & Therapy
Board of Social Work
Board of Chiropractic Examiners
Department of Health
Board of Dentistry
Emergency Medical Services Regulatory Board
Board of Dietetics & Nutrition Practices
Board of Optometry
Nursing Home Administrations Board of Examiners
Department of Veterans Affairs
Board of Medical Practices
Board of Podiatric Medicine
Board of Nursing
Board of Physical Therapy
Board of Barber Examiners
Department of Employment & Economic Development
Explore Minnesota Tourism
Minnesota Zoological Garden Board
Department of Labor & Industry
Pollution Control Agency
Public Utilities Commission
Board of Accountancy
Board of Architecture, Engineering, Land Surveying, Landscape Arch, Geoscience & Interior Design
Department of Commerce
Department of Revenue
Department of Transportation
Indian Affairs Council
Tax Court
Workers Compensation Court of Appeals
Black Minnesotans Council
Chicano Latino Affairs Council
MN State Council on Disabilities
Racing Commission
Board of Water and Soil Resources
Bureau of Mediation Services
Asian-Pacific Minnesotans Council
Department of Administration
Minnesota Management and Budget
Health Professional Services Program
Ombudsperson for Families
Capitol Area Architectural and Planning Board
MN Sentencing Guidelines Commission
Ombudsman for Mental Health & Developmental Disabilities

POLICY REQUIREMENTS

Amateur Sports Commission
Minnesota State Arts Board
Office of Administrative Hearings
Department of Human Rights
Gambling Control Board
Department of Corrections
Office of Higher Education
Department of Education
Perpich Center for Arts Education
MN State Academies
Department of Public Safety
Department of Natural Resources
Department of Human Services
MNsure
Board of Animal Health
Department of Agriculture

RESPONSIBILITIES

Agencies are responsible for:	• Developing protocol for access to data contained in Human Resource Systems • Developing protocol for access by data subject to information contained in Human Resource Systems • Developing protocol for ensuring that MN.IT is notified if access to Human Resource Systems must be inactivated or terminated • Developing protocol for responding to reports of violation of this policy • Disseminating, implementing and enforcing this policy • Obtaining signed acknowledgement from each employee subject to this policy and keeping it in the personnel file.
MMB is responsible for:	Updating this policy as necessary.

FORMS

ACKNOWLEDGEMENT

I acknowledge that I have received and read the Human Resource Systems Data Protection Policy. I understand the requirements of this Policy and acknowledge that I am responsible for complying with this Policy. I understand that if I fail to comply with this Policy, I may be subject to disciplinary action, up to and including discharge.

Dated: _____

Signed: _____

Contacts	Enterprise Human Resources
References	“Data Practices for Personnel Records”, MMB.