Updated: Oct. 29, 2024

Guidance for AI Use in HR-related Work

Considerations regarding AI summarization, generative AI, and other emergent AI tools when engaging in HR work, or with any sensitive or proprietary information.

I. Introduction

This guidance document outlines suggested procedures for the use of artificial intelligence (AI) tools (such as meeting summarization and generative AI technologies). The goal is to ensure the responsible and ethical use of these technologies, particularly within or adjacent to the domain of human resources in which internal, sensitive, and restricted data, including confidential and proprietary information, are frequently handled.

A. Purpose

1. Define the acceptable use of AI.
2. Protect internal, sensitive, restricted and proprietary data from unauthorized access or misuse.
3. Ensure compliance with relevant laws and regulations.
4. Promote transparency and accountability in the use of AI technologies.

B. Scope

1. All faculty, staff, student employees, and third-party vendors/contractors who use AI technologies in any human resources-related work activity that pertains to individuals. Examples include but are not limited to:

    a) Recruitment decision-making
    b) Performance Management
    c) Accommodations, Discipline, and Leave
    d) Title and compensation changes

2. Regardless of job title, all departments and functions, employees, students, and volunteers that handle human resources, sensitive, or proprietary information.

II. Definitions

A. See definitions of AI Technologies: Generative AI services at UW–Madison

B. See Types of data

1. Public

    a) Data should be classified as public prior to display on web-sites or once published without access restrictions; and the unauthorized disclosure, alteration or destruction of that data would result in little or no risk to the University and its affiliates.

2. Internal

    a) Data should be classified as internal when the unauthorized disclosure, alteration, loss or destruction of that data could result in some risk to the University, affiliates, or research projects. By default, all Institutional Data that is not explicitly classified as Restricted, Sensitive, or Public data should be treated as Internal data.

3. Sensitive

    a) Data should be classified as Sensitive when the unauthorized disclosure, alteration, loss or destruction of that data could cause moderate level of risk to the University, affiliates or research projects. Data should be classified as Sensitive if the loss of confidentiality, integrity or availability of the data could have a serious adverse effect on university operations, assets, or individuals.

4. Restricted

    a) Data should be classified as Restricted when the unauthorized disclosure, alteration, loss or destruction of that data could cause significant level of risk to the University, affiliates or research projects. Data should be classified as Restricted if protection of the data is required by law or regulation or UW-Madison is required to self-report to the government and/or provide motive to the individual if the data is inappropriately accessed.

    b) Proprietary: Data that is classified as proprietary is also classified as Restricted data.

III. Acceptable Use

A. Use of UW–Madison provided AI applications (including, but not limited to, automated text summarization, natural language processing tools, or any AI-driven summarization software) is acceptable when drafting non sensitive documents and communications; for example:

1. Drafting non sensitive documents and communications such as HR-related emails
2. Drafting policies
3. Writing general newsletters
4. Getting support for with writing job postings
5. Creating team building activities, or
6. Creating process improvements of tasks through the use of automation that is only using public data and does not pertain to individual employees or candidates.

IV. Discouraged Use

A. Rationale for discouraged use specifically of AI Summarization Tools: The use of AI summarization tools in HR contexts poses risks related to:

1. Data Privacy: Potential exposure or misuse of internal, sensitive or restricted information.
2. Fairness and Accuracy: Risk of misinterpretation or oversimplification of complex human factors that could lead to biased or unfair decisions.
3. Confidentiality: Compromise of confidential discussions and decisions that could impact the university or its employees.
4. See prohibited use and relevant policies for more information.

B. Thus, discouraged use includes:

1. Certain HR Meetings (e.g. workforce relations issues, confidential matters)

2. Use of AI for anything related to employee performance or any matters that contain employee identifying information (PII), including medical information, or student information (as students and as student employees).

3. Other Human Resources activities such as Workforce Relations (investigations, FMLA, accommodations, and other leave that is protected by law, regulation or other policy).

a) Entering any sensitive, restricted or otherwise protected data – including hard-coded passwords – into any generative AI tool or service (see UW-523 Institutional Data and SYS 1031 Data Classification and Protection);

b) Using AI-generated code for institutional IT systems or services without review by a human to verify the absence of malicious elements (see UW-503 Cybersecurity Risk Management);

c) Using generative AI to violate laws; institutional policies, rules or guidelines; or agreements or contracts (see Regent Policy 25-3 Acceptable Use of Information Technology Resources).

V. Important Considerations

A. Employees using AI generation tools are accountable for content created by those tools.

B. Employees are encouraged to engage in manual review, etc. to ensure that all content accurately reflects what is intended with respect to data privacy, safety and security.

VI. Data Privacy, Safety, and Security policies

A. UW-523 Institutional Data
B. UW-504 Data Classification
C. UW-500 Release of Wiscard ID Photos to Campus Software Applications
D. UW-517 University Directory Service (UDS) Responsible Use
E. UW-2007 Disability Documentation and Confidentiality
F. HIPAA Security Program
G. UW-711 Academic Staff Personnel Files
H. UW-4000 Export Controls
I. SYS 1031 Data Classification and Protection
J. SYS 1040 Privacy
K. Regent Policy 25-3 Acceptable Use of Information Technology Resources
L. UW-870 Access to Electronic Files
M. Regent Policy 25-3 Acceptable Use of Information Technology Resources
N. UW-6060 Distribution of Facility Data, Documents, and Graphics Information
O. UW-503 Cybersecurity Risk Management
P. SYS 1039 Risk Management
Q. UW-124 HIPAA Security Risk Management
R. UW-146 Sexual Harassment and Sexual Violence
S. Regent Policy 25-3 Acceptable Use of Information Technology Resources

VII. Compliance with Legal and Regulatory Requirements

A. Legal Compliance: All users must comply with FERPA, HIPAA, GDPR, CCPA and all other applicable laws and regulations.

B. Regulatory Compliance: All users must also ensure they are in compliance with and adhere to all industry-specific regulations they are beholden to.

C. Departments with high risk in legal or regulatory compliance may consider more strict guidance.

VIII. Risk Management

A. Risk Assessment: Cybersecurity Risk Management Implementation Plan

B. Mitigation Strategies

1. AI systems are known to demonstrate biases, and these can vary from system to system based on their training sets and inputs from users. It is critically important to monitor the output/results of AI systems for bias.

2. If AI is used to generate content, results, or analysis it is important to disclose that detail with those it is being shared with.

3. Meeting hosts should never use AI tools to automatically distribute meeting summaries to all participants.

    a) Meeting hosts should turn off summarization for HR meetings. (Transcripts can still be used, provided that they are vetted prior to sharing with others.)

    b) Meeting hosts are permitted to use the summarization product provided the results are not shared with others. See guidance ("Public Records and Records Management").

    c) If you use AI summarization in an HR meeting and share that summary, your summary is subject to Open Records Law, unless exempt under this law (e.g., staff management planning).

C. Incident reporting: Any member of the UW–Madison community who learns of a potential breach of data protection or confidentiality—including through the use of generative AI—must report the incident.

1. UW-509 Incident Reporting and Response

2. SYS 1033 Incident Response
3. UW-131 Reporting of HIPAA Incidents and Notifications in the Case of Breaches of Unsecured Protected Health Information

IX. Contact Information

A. Employees seeking guidance should talk to their HR leader or IT directors who can provide or obtain additional information from DoIT as needed.