

## EXECUTIVE SUMMARY

### AI Usage Policy

As Artificial Intelligence (AI) usage accelerates in all our lives, especially Generative AI, it is imperative that the City of Pocatello get in-line with the technology by establishing a basic AI Usage Policy for City employees.

AI power and usage is growing exponentially throughout the cyberspace and City employees are already using it where they can. Additional usage of AI has been requested by different City departments to better analyze various data, and the Mayor has asked that a basic policy be established to ensure City employees understand the necessity to validate all AI outputs from various systems.

One of the biggest nuisances of AI is what is referred to as data hallucinations. Data hallucination is when incorrect or misleading output is generated by an AI model and is presented as factual. These hallucinations can range from innocent, such as using the wrong name of a City that is referenced; to mission impacting, such as miscalculating budget entries that could lead to an incorrect tax ask. All hallucinations can lead to the loss of the City's integrity with its citizens, employees, or other constituents and /or its counterparts across Idaho or even at the federal level.

The AI Usage Policy that is being presented is a simple placeholder policy that reminds City employees that in the end, they are ultimately responsible for the accuracy of all products that they produce and attach their or the City's name to.

## **AI Policy for City of Pocatello Employees**

### **- Purpose:**

This policy provides guidelines for the responsible use of Artificial Intelligence (AI) tools by City of Pocatello employees. Its goal is to promote transparency, accuracy, accountability, and ethical standards in public service operations supported by AI technologies.

### **- Use of AI Tools**

- Employees may use approved AI tools to enhance productivity, support decision-making, and assist with administrative tasks.
- AI use must comply with all existing laws, regulations, and ethical standards relevant to public sector operations.

### **- Validation of AI Outputs**

- **Mandatory Review:** All outputs generated by AI tools must be reviewed and validated by the employee before use or dissemination. This includes but is not limited to reports, analyses, communications, data interpretations, and public-facing materials.
- **Accuracy Check:** Employees are responsible for verifying the correctness, completeness, and relevance of AI-generated content. If needed, external sources or subject matter experts should be consulted.
- **Accountability:** AI-generated work products are subject to the same standards of quality and integrity as those produced manually. Final responsibility lies with the employee.

### **- Privacy and Security**

- Employees must avoid entering sensitive, confidential, or personally identifiable information into AI tools unless explicitly permitted and secure.
- Any data used with AI systems must comply with city data protection protocols.

### **- Training and Oversight**

- Employees using AI tools are required to complete periodic training on best practices, risks, and ethical considerations related to AI.
- Departments must maintain oversight of AI use and report any issues or concerns to the city's Chief Information Officer or designated compliance officer.

- **Operational Guidance**

- The Information Technology (IT) Department, working with other departments, will develop and update a living AI User Guide that will be adjusted periodically as AI technologies progress over time.

## **Executive Summary**

### **Personal Device Use for Multi-Factor Authentication and Timekeeping into City Systems**

The City of Pocatello requires certain employees, including, but not limited to Police and Fire Department employees, to use personal mobile devices for multi-factor authentication (MFA) when accessing secure systems, including the Spillman law enforcement database. These systems may require MFA via an authenticator app on a mobile device, e.g., smartphone, and not offer any alternative for MFA such as a hard token device. The only way individuals who are required to access these systems as a part of their jobs can access them is via a mobile device.

Additionally, some users may prefer to use their phones for accessing and inputting information into the City's employee timekeeping system.

#### **Legal and Operational Justification**

- De Minimis Use: Under the Fair Labor Standards Act (FLSA) and Idaho law, using a personal phone briefly to receive MFA codes and for timekeeping purposes is considered *de minimis*—too minor to require compensation or reimbursement.
- Privacy Protected: Use is limited strictly to receiving MFA login codes (e.g., via SMS or authenticator app) and timekeeping. This does not constitute general work on a personal device. The City does not access, monitor, or install software on devices used solely for this purpose.
- Public Records Compliance: Use of a personal device for MFA alone does not subject the phone to public records requests under the Idaho Public Records Act unless the device is also used to conduct other City business.

#### **No Alternative for Certain Roles**

- The Spillman system requires MFA via a smartphone and does not support hardware tokens or alternative methods.
- Therefore, the ability to use a personal mobile device for MFA is now a condition of employment for all positions requiring Spillman access.
- It is anticipated that in the future other mission-essential systems will likewise only permit MFA access via a smartphone or similar device and this policy will apply to those systems/positions as well.

# **Personal Device Use for MFA and Timekeeping into City Systems**

## **Policy**

### **A. Purpose**

This policy establishes the conditions under which personally owned mobile devices may be used for limited or authorized City business. It ensures compliance with cybersecurity standards, data security regulations, and the Idaho Public Records Act (Idaho Code § 74-101 et seq.), while maintaining operational continuity through secure authentication methods such as multi-factor authentication (MFA).

### **B. General Policy**

#### **1. Prohibited by Default**

Personal devices (phones, laptops, tablets) may not be used to conduct City business unless specifically permitted under this policy.

#### **2. Permitted Uses**

Personally owned devices may be used for:

- Secure access to City email, calendar, or collaboration tools;
- Receiving emergency or time-sensitive alerts;
- Participating in MFA to access secure City and State of Idaho-required systems;
- Voluntary access into the City's approved timekeeping system

#### **3. Required Use for MFA**

Positions requiring access to the Spillman system, or any other secure platforms protected by authenticator app only MFA, must use a cell phone or smart device capable of receiving authentication codes.

- Not all employees are issued a City-provided phone.
- In these cases, a personal mobile device must be used for MFA.

### **C. Exception – De Minimis Use for MFA**

Use of a personal device strictly for receiving MFA login codes (e.g., SMS, authenticator app, push notification) is considered *de minimis* and does not qualify as business use.

This limited exception:

- Requires no written “bring your own device” (BYOD) authorization;
- Does not entitle the employee to City reimbursement or IT support;
- Does not subject the personal device to records requests under Idaho law, unless other City work is conducted on the device.

Employees using personal phones for MFA:

- Must secure the device with a passcode or biometric lock;
- May not use the device for other City-related business unless authorized under full BYOD.

### **D. Voluntary Use of Personal Devices for Timekeeping Purposes**

Employees may also choose to access the City-authorized timekeeping system from a personal device (e.g., smartphone or tablet) for convenience. This use is considered voluntary and *de minimis* and does not:

- Qualify as formal City business use of a personal device;
- Trigger reimbursement or IT support from the City;
- Require formal BYOD authorization;
- Subject the phone to public records requests;
- Change the employee's rights or obligations under this policy.

City-provided alternatives (e.g., desktop login or physical timeclock) will remain available to all employees. No employee will be required to use a personal device for timekeeping purposes. Employees who voluntarily use a personal device for timekeeping must:

- Access the system through a secure, City-approved app or web portal;
- Maintain basic device security (passcode/biometric lock).

DRAFT

## Internal Steps Necessary:

### 1. Job Description Reclassification (HR)

Job descriptions will need to be updated to reflect that the use of a personal mobile device for MFA is now part of the responsibilities for specific positions, especially those accessing systems like Spillman.

This update should clarify the following:

- **Requirement:** That employees in these roles are required to use their personal cell phones (or a smart device) for MFA to access City systems.
- **No Additional Compensation:** There will be no additional compensation for using a personal device for MFA purposes. This is considered a minimal (de minimis) use of their personal device.
- **Clear Impact on Employment:** The reclassified job description should specify that refusal to use a personal mobile device for MFA could result in the employee being unable to access critical systems and, therefore, unable to perform their job duties.

### 2. Employee Notification and Acknowledgment (HR and DHs)

Formal communication will need to be had with each employee in the affected roles, notifying them of the new requirement to use a personal cell phone for MFA. This communication should include:

- **Description of the Requirement:** The exact nature of the requirement (i.e., the use of a personal mobile device solely for MFA).
- **De Minimis Use:** A clear explanation that the use of the device for MFA is de minimis and does not constitute broader work-related use or necessitate reimbursement or IT support.
- **No Additional Compensation:** Reiterate that the City will not compensate employees for using their personal devices for MFA purposes.
- **Consequences of Non-Compliance:** Clarify that failure to comply with this requirement may result in the inability to perform essential job functions and could lead to disciplinary action.

### 3. Signature and Acknowledgment (HR)

Employees will be required to sign an acknowledgment indicating that they understand and agree to the new requirement of using their personal mobile device for MFA. The signature will be obtained on the following document:

- **Updated Job Description:** Have the employee sign off on the revised job description that includes the MFA requirement.
- **Ensure that employees have ample time to review the policy before signing and that you provide an opportunity for them to ask any questions.**

### 4. Documentation

Once signed, the updated job descriptions should be kept in the employee's personnel file for compliance and future reference.