Acceptable Use of IT Resources with Acknowledgement Form

1. Purpose
   This document is a summary of IT policies pertaining to acceptable behavior, and is not a comprehensive list of all requirements. Please refer to any and all references acknowledged within this document for additional information. This document is to be used for onboarding of all employees and identifies the rules of behavior for state employees and contractors unless an exception is authorized by a Department head. These rules describe their responsibilities and expected behavior with regard to information and IT resources usage. All state employees and contractors shall sign an acknowledgment indicating that they have read, understand, and agree to abide by the rules of behavior before they are authorized to access any state information or IT resource.

2. Policy
   Acceptable Use of IT Resources applies to the following controls found within the Information Security Policy.
   a. Information Security Policy
      - Identify
        - 1.7
      - Protect
        - 2.1, 2.4.15, 2.5, 2.6.1, 2.8, 2.9.3.4, 2.9.5.3, 2.13, 2.16.5, 2.18, 2.19
      - Detect
        - 3.1, 3.2
      - Respond
        - 4.6
      - Recover
        - 5.7
   b. Information Security Policy – Appendix A
      - Access Control (AC)
        - AC-8 – System Use Notification
        - AC-11 – Session Lock
        - AC-17 – Remote Access
      - Awareness and Training
        - AT-2 Security Awareness Training

- Configuration Management (CM)
  - CM-7 – Least Functionality
  - CM-10 – Software Usage Restrictions
  - CM-11 – User-Installed Software
- Contingency Planning
  - CP-8 – Telecommunications Services
  - CP-9 – Information System Backup
- Identification and Authentication
  - IA-5 - Authenticator Management
- Incident Response
  - IR-6 - Incident Reporting
- Media Protection (MP)
  - MP-4 Media Storage
  - MP-5 Media Transport
  - MP-6 – Media Sanitization
  - MP-7 – Media Use
- Physical and Environmental Protection
  - PE-8 – Visitor Access Records
- Planning (PL)
  - PL-4 – Rules of Behavior
- System and Communications Protection
  - SC-7 Boundary Protection
- System and Information Integrity
  - SI-3 Malicious Code Protection

3. Relevant Policies

a. Information Security Policy
b. Information Security Policy – Appendix A
c. Identification and Authentication Policy
d. Electronic Mail Policy
e. Social Media Policy
f. Social Media Guidelines
g. Social Media Request Form
h. Mobile Device Management Policy
i. Mobile Device User Agreement Form

4. Acceptable Uses for IT Resources:

As stated in 2-2-103(1)(2), MCA,

> A public officer, legislator, or public employee shall carry out the individual's duties for the benefit of the people of the state.
>
> A public officer, legislator, or public employee whose conduct departs from the person's public duty is liable to the people of the state and is subject to the penalties provided in this part for abuse of the public's trust.

Device Use

- Access to IT resources in the form of devices and facilities are issued in accordance with performing assigned duties for the benefit of the people of Montana. Users of State of Montana IT resources and facilities are personally responsible for their conduct and behavior in the use of assigned resources.
- Agencies may allow incidental, non-excessive personal use of IT resources at their discretion. The agency must have a policy that describes this use.
- There is no expectation of privacy while using the State IT resources. All activity can be logged, monitored, and reviewed.
- Users are expected to comply with all applicable IT-related contractual and license agreements. Users should check with their agency IT division for guidance.
- Work-related files and electronic information shall be stored on State approved storage services to ensure the document(s) are backed up.
- Use of unapproved cloud-based services for data storage, transfer, etc. is prohibited.
- Employees must never attempt to gain access to, disclose, or remove any user ID, information, software, or file that is not their own and for which they have not received explicit authorization to access.
- Users shall not interfere with, encroach on or disrupt others' use of the State's shared IT resources. For example, by
  - playing computer games, streaming non-work related video, sending excessive messages, attempting to crash or tie up a State computer.
  - damaging or vandalizing State computing facilities, equipment, software, or computer files.
- Users shall not knowingly transfer or allow to be transferred to, from or within the agency, textual or graphical material commonly considered to be child pornography or obscene as defined in 45-8-201(2), MCA.
- All hardware and software, including downloaded software, shall be authorized, purchased and installed by authorized agency staff prior to use.

- Users shall not connect *non-State* owned storage media (USB storage devices, external or internal hard drives), including *personal* mobile devices (iPads, Kindles, smartphones, etc.) to the workstation or internal network
- IT resources must not be used for private, commercial, or political purposes.
- Remote Access to the State's internal network must be authorized by a supervisor and utilize State approved software.
- Users shall report missing or stolen IT hardware immediately to their supervisor and agency ServiceDesk.
- Users shall notify their agency's Service Desk and supervisor in the event of a security incident or if the IT device is acting unusual, e.g. slow performance or response times, unexpected pop-up advertisements, etc.
- Devices must be locked before leaving them unattended. Users must log off of devices at the end of the day unless permission has been received to run a job or process.

Passwords

- Passwords should be strong, with a minimum of 8 characters. Users are required to have a combination of upper and lower case with special and numerical characters contained in their passwords.
- Passwords must never be shared with *ANYONE.*
- Personal information must never be used in a password (e.g., SSN or date of birth).
- Users must secure their password at all times. Passwords are not to be written down (e.g., taped to monitor or under keyboard).
- Additional policy requirements for passwords are contained in the Identification and Authentication Policy .

Internet

Internet usage is provided for the opportunity it gives state employees and contractors to accomplish their job duties.

- Shall be used for conducting state business, however,
  - Agencies may allow incidental, non-excessive personal use of internet at their discretion. The agency must have a policy that describes this use.
- Agency system administrators, management, and appropriate Department of Administration personnel can monitor Internet usage for planning and managing network resources, performance, troubleshooting purposes, or if abuses are suspected.
- Read the following for additional policy requirements – see section CP-8: [Information Security Policy – Appendix A (Baseline Security Controls)]

Electronic Mail

- Shall be used for conducting state business, however,
  - Agencies may allow incidental, non-excessive personal use of Electronic Mail at their discretion.
- Email is considered public record. Employees should have no expectations of privacy. (See https://sos.mr.gov/records/defined for additional info.)
- Never click on attachments or links to any email from an unknown person or company. Forwarded such suspicious email to your agency service desk or to the DOA-SITSD ServiceDesk immediately (servicedesk@mt.gov).
- State email accounts must not be used to sign up for non-work related website accounts, mailing lists, etc.
- Personal email account(s) shall not be used for work-related business.
- Shall not be used to circulate chainmail, spam, etc.
- Shall not send sensitive information to other parties unless authorized by agency and appropriately encrypted.
- Shall not send inappropriate materials such as:
  - Sexually offensive, explicit
  - Harassing or discriminatory
  - Gruesome, violent, or sadistic
- Read the following for additional policy requirements: Electronic Mail Policy

Social Media

- If authorized, can only be used for work-related purposes
- Work-related communications should be professional and consistent with the agency's mission and the position's responsibilities,
- Read the following for additional policy requirements: Social Media Policy, Social Media Guidelines, Social Media Request Form

Mobile Device Management

- Granting of Mobile Device access to State of Montana IT resources shall be managed by agency IT staff.
- State information managed from a mobile device requires authentication, which must include either a device passcode or user password.
- Passcodes are required to follow the state policy for passwords. This includes biometrics. See previous section for link to Password Policy.
- Jailbroken or "rooted" devices will not be allowed to enroll in the enterprise MDM solution.
- If a device becomes compromised while it is enrolled, state information will be removed and the device will not be allowed access to the State network or State information. Access will not be restored until the device has been wiped or receives a factory reset.

- Read the following for additional policy requirements: Mobile Device Management Policy, Mobile Device User Agreement Form

Security Training

- The State of Montana provides security awareness training to new employees, as well as annual security training to all other staff members including managers, senior executives, and contractors. This training is managed by the employee's agency.

Sensitive Information

- Users shall refer to relevant State statutes and their agency's policies for guidance on categorizing State information.
- State of Montana Level 2 and 3 data classifications must be appropriately handled, marked, stored, and transmitted. See Data Classification policy and guideline.
- Ensure any personally identifiable information is saved to an appropriate location (e.g. encrypted location).
- Must not be stored, transferred, or copied to unauthorized locations.
- Shall utilize the State of Montana File Transfer Service or OneDrive for Business or Enterprise Approved encrypted email for any transfer needs of sensitive information.
- Shall only be stored on State-owned portable devices and portable storage if there is a business requirement.
- If position requires access to sensitive information, an Elevated Privileges Acknowledgement form (see attached example) will be signed by designee and approved by management prior to being granted access.
- Shall not be transported outside of the United States on portable devices or portable storage.
- Protect IT devices containing sensitive information (e.g. flash drives, computers, cell phones, etc.) until the device is destroyed or sanitized using approved tools or equipment.
- Report lost, stolen or compromised information to immediate supervisor and agency Information Security Manager.
- Agree to follow all visitor access procedures.

Multi-Factor Authentication

- Multi-Factor authentication is the state standard for access to State of Montana computer systems. It is achieved through use of RSA physical fob or soft token.

- The agency in partnership with the State Information Technology Services Division (SITSD), is responsible for distributing and managing RSA fobs. One

fob will be issued to each employee or service provider who requires it for their position along with their User ID.

- Fobs are not to be shared with other individuals.
- Employees and service providers are responsible for the physical security of the fob at all times in order to prevent unauthorized access.
- Lost, stolen or misplaced fobs must be reported immediately by calling the Agency Service Desk or SITSD Service Desk at (406) 444-2000. The employee's or service provider's manager must request a replacement fob or temporary passcode.

4. Compliance

Compliance is shown by implementing this Enterprise Acceptable Use of IT Resources as described above. Policy changes or exceptions are governed by the Procedure for Establishing and Implementing Statewide Information Technology Policies and Standards. Requests for a review or change to this document can be made by submitting an Action Request form. Requests for exceptions are considered by submitting an Exception Request form to DOA_SITSD. Changes to policies and standards will be prioritized and acted upon based on impact and need.

APPENDIX A

(add Agency)
(add Division)

SAMPLE - Rules of System Usage Acknowledgement Form

I _____ have read the **(add Agency and State)** policies and procedures regarding the use of information systems and I agree to comply with all terms and conditions. I agree that all information system activity conducted while doing **(add Agency)** business and being conducted with **(add Agency)** resources is the property of the State of Montana.

I understand that any information system to which I have access, can only be used for its intended purpose. I also agree to avoid the disclosure of any protected information to which I have access.

I understand that **(add Agency)** reserves the right to monitor and log all information system activity including email and Internet use, with or without notice, and therefore I should have no expectations of privacy in the use of these resources.

If my position requires a background check, I understand that the results of this background check can affect my employment. (Identified by agency HR staff)

_____ Yes, this position requires a background check

_____ No, this position does not require a background check.

Signed _____

Position Title _____ Position Number

_____ Date _____

NOTE: This form will be signed by each **(add Agency)** *employee on an annual basis.*

APPENDIX B

(add Agency)
(add Division)
SAMPLE - Rules of System Usage for Users with Elevated Privileges
Acknowledgement Form

A. INTRODUCTION

I, _____, understand that as an employee of the _____, I may have access to several categories of confidential data and information. This data and information may be generated by me or provided to me by others regarding individuals and entities in either oral and written form through a variety of communication mediums, including during in-person or telephonic conversations, by electronic or paper documentation, or by other means during interactions with others from within the Department, from other agencies, or with individuals or entities outside of state government. I understand the importance of maintaining the confidentiality of this data and information to protect the privacy rights of individuals and entities, including employees and the general public, and to protect the State and me from possible liability, penalties, and criminal charges for unlawful disclosure. Because of these responsibilities, I understand the need for reading, understanding, and signing this Acknowledgement.

B. FEDERAL AND STATE TAX INFORMATION

I understand the following:

1. I may have access to Federal Tax Information (FTI) and State Tax information as defined in footnote 1 below.
2. Tax returns or tax information disclosed to each user may be used only for a purpose and to the extent authorized by the data manager in connection with the processing, storage, transmission, and reproduction of tax returns and return information; the programming, maintenance, repair, testing, and procurement of equipment; and providing other services for purposes of tax administration.
3. Further disclosure of any tax returns or tax information for a purpose or to an extent unauthorized by the data manager for these purposes constitutes a felony, punishable upon conviction by a fine of as much as $5,000, or imprisonment for as long as five years, or both, together with the costs of prosecution (Internal Revenue Code (IRC) section 7213).
4. Further inspection of any tax returns or tax information for a purpose or to an extent not authorized by the data manager for these purposes constitutes a misdemeanor, punishable upon conviction by a fine of as much as $1,000, or imprisonment for as long as one year, or both, together with costs of prosecution (IRC 7213A)

5. Should either unauthorized access or disclosure occur, individually I can be sued by the taxpayer and would be liable for civil damages amounting to a minimum of $1,000 for each act or the actual damages sustained by the taxpayer (whichever is greater) as well as the costs of the court action (IRC 7431).
6. Under Montana law, 15-70-209, MCA; 15-70-344, MCA; and 15-70-351, MCA, a user cannot disclose or disseminate information contained in a statement required under the fuel-tax sections. Making an unauthorized disclosure or unauthorized inspection of information can make the person subject to the disciplinary procedures established by state law, which could include termination from employment.
7. Under Montana law, 15-30-2618, MCA; 15-31-511, MCA; 15-7-310, MCA, a user cannot disclose or disseminate information under these state tax sections. Making an unauthorized disclosure or unauthorized inspection of information can make the person subject to the disciplinary procedures established by state law, which could include termination from employment.
8. If exposure to FTI is expected through my employment position with the Department of _____, I have received awareness training and understand the policies and procedures for safeguarding FTI and the penalties for unauthorized inspection or disclosure of FTI.

C. CRIMINAL JUSTICE INFORMATION

I understand the following:

1. I may have access to criminal justice information as defined in footnote 2 below, via the state network.
2. My access to this information is limited for the purpose(s) outlined in the agreement between the Department of _____ and the government agency providing the information.
3. Criminal history information and related data are particularly sensitive and may cause great harm if misused.
4. Misuse of the system by accessing it without authorization, exceeding the authorization, using the system improperly, or using, disseminating or re-disseminating criminal justice information without authorization, may constitute a state crime, federal crime, or both.

D. PROTECTED HEALTH INFORMATION

I understand the following:

1. I may have access to Protected Health Information (PHI) as defined in footnote 3 below.
2. Maintaining confidentiality of PHI is my legal obligation to State of Montana employees, retirees, and their dependents covered under the State health plan, to the Montana citizens who are covered under a public assistance program, and to the individuals whose PHI is stored in the State's data warehouse.
3. I shall consider as confidential any and all PHI, oral or written, pertaining to individuals, family members/domestic partners, and employees.

4. I am responsible as a Department of _____ employee for maintaining confidentiality of PHI outside of the professional boundaries of this job.
5. I shall use and disclose the minimum necessary amount of PHI to perform my job duties.
6. Uses or disclosures of PHI that are outside of those allowed by the State's policies must be made known immediately to my supervisor.
7. Unintentional failure to comply with the privacy policies of the State or the law regarding PHI may result in sanctions including civil penalties and disciplinary action up to and including termination.
8. Intentional failure to comply with the privacy policies of the State or the law regarding PHI may result in civil penalties and criminal prosecution.

E. CONFIDENTIAL EMPLOYEE DATA AND INFORMATION

I understand the following:

1. I may have access to Confidential Employee Data and Information. That information may include, but is not limited to:
    a. Personal employee information, including a person's address, telephone number, email address, social security number, driver's license number, bank and credit card information, health information, and other identifying information. Although an employee's first and last name is not generally considered confidential, there may be circumstances when an employee's first and last name may be confidential based upon the sensitive nature of their position.
    b. Race, sex, marital status, disability, other demographic information.
    c. Medical records, personal health information including information regarding enrollment in a benefit plan and all information designated as PHI protected under HIPAA, the ADA, or FMLA. Personally identifiable information (PII), such as name, date of birth, or social security number, becomes personal health information to be protected under HIPAA when the PII is combined with the individual's past, present, or future physical or mental health or condition; the provision of health care to the individual; or past, present, or future payment for the provision of health care to the individual.
    d. Genetic information protected under Genetic Information Nondiscrimination Act.
    e. Individual tax and financial information, except state employees' salary or wage information and leave information is not protected. The reason for sick leave is protected.
    f. Pre-employment information, including resumes, applications, reference checks, background checks, credit reports provided according to Fair Credit Reporting Act, question responses, and evaluation notes.
    g. Accident reports and workers' compensation claims.
    h. I-9 forms.
    i. Performance appraisals.
    j. Disciplinary actions and investigation reports, non-public litigation, audit and inquiry information.
    k. Computer system passwords and security codes.

l. Attorney-client communications and attorney work product.
m. Any other information that is designated or marked as confidential by contract or non-disclosure agreements.

2. Individuals may have an expectation of privacy in this Confidential Employee Data and Information.
3. I shall maintain the confidentiality of this data and information, and I may be subject to discipline up to and including termination of employment if I fail to do so.

ACKNOWLEDGEMENT AND ATTESTATION

I understand that it is a condition of my employment to maintain confidentiality of data and information and that I may be subject to consequences indicated if I fail to do so. There may be instances when disclosure of confidential data or information is permitted as required as part of my job duties or as required by law. Prior to any disclosure, I shall contact Department of _____ legal counsel or my supervisor. If I do not know whether certain data or information is confidential and whether or not I may provide it to an individual or requestor, I am expected to ask Department of _____ legal counsel or management whether it is appropriate to disclose the requested data or information before I disclose it. Otherwise, I shall not disclose the confidential data or information.

I understand that if I unintentionally disclose protected information or become aware of another person's unintentional or intentional unlawful disclosure, I must immediately report it to my supervisor or another manager so that steps may be taken to mitigate the disclosure, including to inform the individual whose information was disclosed if required by law, or to recover the information.

I understand and agree that upon termination of my employment, I shall return any confidential information in my possession, and I shall maintain the confidentiality of data and information I have learned after termination of my employment.

I have read this statement in full, have asked and clarified my questions regarding its content and the expectations for me regarding maintaining the confidentiality of data and information, and understand the consequences for failing to protect the confidentiality of data and information. My signature below indicates my agreement to adhere to the requirements of this statement.

Signed _____

Date _____

1 **FTI (IRS Code) -** A taxpayer's identity, the nature, source, or amount of his income, payments, receipts, deductions, exemptions, credits, assets, liabilities, net worth, tax liability, tax withheld, deficiencies over assessments, or tax payments, whether the taxpayer's return was, is being, or will be examined or subject to other investigation or processing.

2 **CJIS Data -** Data considered to be criminal justice in nature to include images, files, records, and intelligence information. FBI CJIS data is information derived from state or Federal CJIS systems.

3 **PHI -** Individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or maintained or transmitted in any form or medium including, without limitation, all information (including demographic, medical, and financial information), data, documentation, and materials that are created or received by the State's health plan, public assistance programs or data warehouse or a Business Associate from or on behalf of the State's health plan or public assistance programs in connection with the performance of services and relates to:

a) The past, present or future physical or mental health or condition of an individual;
b) The provision of health care to an individual; or
c) The past, present or future payment for the provision of health care to an individual;

and that identifies or could reasonably be used to identify an individual and shall otherwise have the meaning given to such term under the HIPAA Privacy Rule. PHI does not include health information that has been de-identified in accordance with the standards for de-identification provided for in the HIPAA Privacy Rule. PHI does not include employment records held by the State in its role as employer.