



**STATE OF MONTANA  
DEPARTMENT OF CORRECTIONS  
POLICY DIRECTIVE**

|  |                                   |
|--|-----------------------------------|
| Policy No. DOC 1.7.7                     | Subject: <b>COMPUTER SECURITY</b> |
| Chapter 1: ADMINISTRATION AND MANAGEMENT | Page 1 of 4 and Attachment        |
| Section 7: Information Systems           | Effective Date: Dec. 1, 1996      |
| Signature: /s/ Mike Batista, Director    | Revised: 03/02/2016               |

## **I. POLICY**

The Department of Corrections administers computer security to prevent the intentional or unintentional modification, destruction, disclosure, or misuse of data and information technology resources, and to remain in compliance with state laws and policy.

## **II. APPLICABILITY**

All divisions, facilities, or programs Department-owned or contracted, as specified in contract.

## **III. DEFINITIONS**

Data and Information Technology Resources – The State mainframe computer; the State's and the Department's mid-range computers and file servers; the Internet and intranet; Local, Wireless, Virtual and Wide Area Networks (LANs, VLANS, WLANs & WANs) and associated equipment; microcomputer hardware and software, printers and other peripherals; facility resources related to computing, electronically stored data, email services, and other related resources.

Data Owner – The entity that can authorize or deny access to certain data and is responsible for its accuracy, integrity, and timeliness.

Department Employee – A person employed by the Department of Corrections who has attained permanent status or is eligible to attain permanent status, as provided in 2-18-601, MCA; volunteers, interns, temporary and short term workers; this term does not include service providers.

Password – An alphanumeric combination of characters unique to individual users that allows access to a specific computer, network or computer system.

Service Providers - This term includes contracted persons or other vendors providing service whose assignment is primarily on Department premises, e.g. facility or program office.

Temporary Employee – An employee who is designated as temporary by an agency for a definite period of time not to exceed twelve months; performs temporary duties or permanent duties on a temporary basis; is not eligible for permanent status; is terminated at the end of the employment period; or is not eligible to become a permanent employee without a competitive selection process.

User ID – Used generically to refer to CI number, login ID, ACF2 ID, user account, or any other term used to describe a user's unique identifier which is used to grant rights and privileges on a computer, computer system or network. User IDs are never reused.

## **IV. DEPARTMENT DIRECTIVES**

### **A. General**

**Subject: COMPUTER SECURITY**

1. The Department has delegated its statutory authority for the security of data and information technology resources to the Information Technology (IT) Division.
2. The IT Division will appoint a security officer(s) to handle daily activities related to providing staff access to the systems and data needed to perform their jobs.
3. Department data, in general, belongs to the Department's programs; the IT Division functions as the "caretaker" of data for programs by granting and restricting access on behalf of the owners of each set of data.
4. Each division, facility or program will coordinate security access requirements to information systems with the IT Division. The identified data owner must approve access requests from another program before access is granted.
5. The security officer may develop and implement additional procedures to protect the integrity of, and access to, Department data and information technology resources.
6. The IT Division grants data access on a "most restrictive" or "least rights" basis; users are granted the lowest level of access possible to accomplish their job functions.
7. The Office of Human Resources (OHR) will notify the security officer via the IT Service Desk whenever an employee changes positions within the Department and request appropriate changes to the employee's or service provider's access rights. OHR will also notify the IT Service Desk when an employee or service provider discontinues employment or is terminated so access to systems and data may be adjusted.

**B. User ID and Passwords**

1. Each employee, service provider or other individual allowed access to any Department information system or connected to the Department network will be assigned a User ID and password; applications that run on these systems may require a separate User ID and password. By accessing Department IT resources, the individual is agreeing to follow Department policy.
2. User IDs and passwords grant individual rights that vary depending upon job requirements; i.e., employee "A" may have a User ID that allows access to all parts of the Offender Management Information System (OMIS) while employee "B" has a User ID that grants access to only certain parts of OMIS.
3. Employees and service providers must protect the confidentiality of their User ID and password, may not share the information, and may not write the information where others could find them.
4. Individuals will lock their account when leaving a computer and will not allow others access to their account unless approved by the IT Division.
5. If employees or service providers violate this policy, computer rights will be immediately terminated. Supervisors may not reinstate individual computer rights before assuring the security officer that steps have been taken to prevent further violations.

6. The IT Division may grant emergency access to an absent employee's or service provider's data and/or email account if approved by the appropriate supervisor from the program "owning" the data; requests will be made in writing with a limited time frame and be evaluated on a case-by-case basis by the security officer.

### **C. RSA Two Factor Authorization**

1. Two factor authorization is the state standard for access to State of Montana computer systems. It is achieved through use of RSA fobs.
2. The IT Division, Network Services Bureau (NSB), 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.
3. Fobs are not to be shared with other individuals.
4. Employees and service providers are responsible for the physical security of the fob at all times in order to prevent unauthorized access.
5. Lost, stolen or misplaced fobs must be reported immediately by calling the Service Desk at (406) 444-4234. The employee's or service provider's manager must request a replacement fob or temporary passcode.
6. If a replacement fob is needed, the Department will pay for the first replacement fob. The employee or service provider must pay \$50 for each replacement fob thereafter.
7. For emergency situations where the employee or service provider does not have immediate access to their fob, the employee's or service provider's manager may contact the Service Desk to request a temporary one day passcode to gain access to the network. Temporary pass codes will not be issued longer than a 12-hour period.
8. Fobs for temporary employees will be issued to and managed by their direct supervisor. The supervisor is responsible for accounting for the fob. When the temporary employee leaves employment, the supervisor will immediately notify the Service Desk so they can disassociate that fob in the system. The supervisor will maintain physical control and accountability of the fob until it is reassigned to the next temporary employee.
9. When a permanent employee leaves the Department, the employee's supervisor is responsible for that fob until it is returned to the Service Desk or reissued to the employee taking the vacated position.

### **V. CLOSING**

Questions concerning this policy should be directed to the Department's Chief Information Officer (CIO), or designee.

### **VI. REFERENCES**

- A. 2-15-112, MCA; 2-15-114, MCA; 2-17-534, MCA
- B. 1-0250.00 Montana Operations Manual

Subject: **COMPUTER SECURITY**

- C. *ENT-SEC-063, ENT-SEC-072; Enterprise IT Policy*
- D. *DOC Policies 1.7.3 Data Quality; 1.7.6 Unlawful Use of IT Resources; 1.7.9 Acceptable Use of IT Resources*

## **VII. ATTACHMENT**

[IT Consent](#)