



**D. Rico Munn**  
**Executive Director**

## **CYBER SECURITY POLICY**

**Policy Number:** 2008-DORA-ITS-002

**Effective Date:** 02/08/2008

**REFERENCE:** The Department of Regulatory Agencies (DORA) will adhere to the State Cyber Security Program Policy (CSPP) CSPP-001. This policy requires that all state agencies shall maintain a Cyber Security Program to control risks associated with access, use, storage and sharing of sensitive citizen and State electronic information and document the program details in an Agency Cyber Security Plan (ACSP).

### **I. PURPOSE OF POLICY**

To ensure that DORA prohibits unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse or theft of sensitive electronic information assets.

### **II. DEFINITIONS**

- A. Private Information** means personal information (any information concerning a person, which because of name, number, personal mark or other identifier, can be used to identify such person) PLUS one or more of the following:
- i.** Social security number, or
  - ii.** Driver's license number or non-driver identification card number, or
  - iii.** Account number, credit or debit card number, in combination with required security code, or password which would permit access to an individual's financial accounts, or
  - iv.** Protected Health Information (PHI) as defined in HIPAA regulations, or
  - v.** "Private information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.
- B. Sensitive Information** means any information where unauthorized access, disclosure, modification, destruction or disruption of access to or use of such information could severely impact DORA, its critical functions, its employees, third party business partners, citizens of Colorado and/or its customers.

### **III. POLICY**

- A.** Release of public information; Information Technology Services (ITS) will release information only to DORA divisions. Further dissemination of the information will be the responsibility of the division or office. The official custodian for the division or office must determine if the requested information constitutes a public record whose disclosure is statutorily authorized.
- B.** Workstation Security

- i.** All DORA staff, permanent, temporary, or contractor shall have their own network user ID; user IDs will not be shared.
  - ii.** Account passwords will expire every sixty days. Users assume the full responsibility for the security of their passwords.
  - iii.** The same password cannot be used consecutively.
  - iv.** Passwords must be kept confidential and not shared among users.
  - v.** A user must always log on individually under his/her own login ID and password.
  - vi.** All workstations connected to the network will be automatically locked after 30 minutes of inactivity.
  - vii.** Users should log off or lock your computer workstation when they plan to be away from their desk for more than a few minutes (e.g. coffee break, lunch, etc.).
  - viii.** Users should follow common sense information security procedures (e.g. printouts of information should not be left in the printer area for an extended period of time; old printouts should be properly disposed of).
  - ix.** Any access to restricted hardware, software, data or reports without the required permissions is prohibited. Do not “browse” or otherwise access DORA files (network, computer reports, etc) that are not yours and that you do not have the owner’s permission to use.
- C.** Handling, storing and destruction of private and sensitive information: The state Chief Information Security Officer (CISO) has published an emergency interim guideline to all state government concerning the storage of ‘private or sensitive information’. This agency guideline is effective immediately and ONLY pertains to data classified as ‘private or sensitive information’.

#### **IV. IMPEMENTATION RULES**

- A.** It is prohibited for a person, working for or contracting with the Department of Regulatory Agencies, to store state-owned ‘private or sensitive information’ on a personally owned portable computing device. This includes laptop computers, memory sticks, cell phones, PDA’s, CD’s, or USB devices. Approved storage devises are DORA owned servers, workstations, PDA’s, USB, or CD’s provided for staff use. ITS has received and encrypted DORA laptops to comply with the State Cyber Security Office policies.
- B.** It is prohibited for a person, working for or contracting with the Department of Regulatory Agencies, to transmit state-owned ‘private or sensitive information’ electronically without state approved encryption protection. While we are working on providing this, it is prohibited to transmit ‘private or sensitive information’ electronically. The exception to this policy is:
- i.** e-mail transmitted from on premise DORA approved equipment to on premise DORA approved equipment
  - ii.** Information transmitted over the secure FTP i.e. Liberty Imaging, Exam data (Headmaster, Promissor)
  - iii.** Information transmitted to DORA through dial up

- C. If an employee or contractor of this Department is currently storing data on a portable computing device (self-owned or state-owned) that could be defined as state owned 'private or sensitive information', they must inform their immediate supervisor.
- D. All Private or Sensitive information not approved to be stored on the storage device must be *wiped* from those devices using an approved methodology outlined in the Colorado Data Destruction Policy (Policy #P-104A dated February 2004) which can be found at:  
[http://www.colorado.gov/oit/documents/policies/CO\\_Data\\_Destruction\\_Policy\\_02062004\\_Revised.pdf](http://www.colorado.gov/oit/documents/policies/CO_Data_Destruction_Policy_02062004_Revised.pdf)

## V. INCIDENT RESPONSE PROCEDURE

DORA has a published Incident Response Procedure which can be found at:  
<http://dora.state.co.us/Policies%20and%20Procedures/IncidentResponse08302007.doc>

## VI. APPLICABILITY

This policy is applicable to all divisions and offices of the Department of Regulatory Agencies.

## VII. RESPONSIBILITY

It is the responsibility of each person to whom policies or procedures are applicable to become familiar with, and to understand and adhere to departmental policies and procedures. During new employee orientation employees will be instructed on where to find the departmental policies and procedures.



2-8-08

Approved by: \_\_\_\_\_  
D. Rico Munn , Executive Director                      Date