

Effective: 07/01/11

Date: 07/01/11

Adopted: 06/26/11

Last Revised: 05/02/16

**SUBJECT:** Cyber Incident Response Policy

## **PURPOSE**

This policy is established to clarify roles and responsibilities in the event of a cyber incident. The availability of cyber resources is critical to the operation of government and a swift and complete response to any incidents is necessary in order to maintain that availability and protect public and private information.

### **Responsible Executive**

If the incident affects multiple departments, the County Administrator shall be the Responsible Executive. If only one department is impacted, the Department Head shall fill this role. The responsibilities of the executive include, but are not limited to:

- Receiving initial notification and status reports from the Incident Response Manager;
- Consulting with other executives on public notification, involvement of the organization's attorney and notification of law enforcement;
- Preparing and delivering press releases;
- Consulting with other executives and appropriate staff on priorities for response and recovery; and
- Advising the Incident Response Manager on priorities.

### **Incident Response Manager / Co-Manager**

Flathead County designates that the Systems and Security Administrator as the Manager, and the Web Developer as the Co-Manager has responsibility for preparing for and coordinating the response to a cyber incident. Responsibilities include, but are not limited to:

- Developing and testing response plans;
- Being the point of contact should any employee or official believe an incident has occurred;
- Involving the identified technical support to address the incident;
- Notifying the appropriate executive that an incident has occurred if significant;
- Advising executive regarding notification of law enforcement and the county attorney if appropriate;
- Providing information to the individual (s) responsible for notifying the press and public;
- Coordinating the logging and documentation of the incident and response to it; and
- Making recommendations to reduce exposure to the same or similar incidents.

### **Technical Support Staff**

The Information Technology Department shall provide technical support to the Incident Response Manager. Responsibilities include, but are not limited to:

- Training users to recognize and report suspected incidents;

- Assessing the situation and providing corrective recommendations to the Incident Response Manager;
- Helping the Incident Response Manager make initial response to incidents;
- Responding to the incident to contain and correct problems;
- Reporting to the Incident Response Manager on actions taken and progress;
- Participating in review of the incident and development of recommendations to reduce future exposure;
- Consulting with other executives on public notification, involvement of the municipal attorney, and notification of law enforcement;
- Assisting with preparation of press releases;
- Consulting with other executives and appropriate staff on priorities for response and recovery; and
- Advising the Incident Response Manager on priorities.

**Legal Counsel**

The Flathead County Attorney's Office shall provide advice as called upon.