West Texas A&M University™

The Division of Information Technology
University Information Security Standards

NIST CONTROL FAMILY
IDENTIFICATION AND AUTHENTICATION CONTROLS

CONTROL NUMBER	CONTROL NAME	PRIORITY	REVIEW DATE
IR-8	**Incident Response Plan**	**P1**	**07/22/2017**

I. STATEMENT

West Texas A&M University will develop an incident response plan that:

1. Provides WTAMU with a roadmap for implementing its incident response capability;
2. Describes the structure and organization of the incident response capability;
3. Provides a high-level approach for how the incident response capability fits into the overall University;
4. Meets the unique requirements of the University, which relate to mission, size, structure, and functions;
5. Defines reportable incidents;
6. Provides metrics for measuring the incident response capability within the University;
7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
8. Is reviewed and approved by Chief Information Officer.

The Chief Information Officer will distribute copies of the incident response plan to incident response personnel responsible for information system restoration; review the incident response plan; updates the incident response plan to address system changes or problems encountered during plan implementation, execution, or testing; communicates incident response plan changes to organization-defined incident response personnel; and protects the incident response plan from unauthorized disclosure and modification.

II. APPLICABILITY

This Control applies to all West Texas A&M network information resources. The intended audience for this Control includes all information resource owners, custodians, and users of information resources.

III. IMPLEMENTATION

WTAMU has an incident management policy that describes the requirements for dealing with computer security incidents including prevention, detection, response, remediation, and reporting.