

Intrusion Detection Standard

Revision Date:

1. Purpose: Intrusion detection provides two important functions in protecting information resources:

- Feedback: information as to the effectiveness of other components of the security system. If a robust and effective intrusion detection system is in place, the lack of detected intrusions is an indication that other defenses are working.
- Trigger: a mechanism that determines when to activate planned responses to an intrusion incident.

2. Scope: The EPCC Intrusion Detection Standard applies to all individuals that are responsible for the installation of new Information Resources, the operations of existing Information Resources, and individuals charged with Information Security.

3. Description: Intrusion detection plays an important role in implementing and enforcing an organizational security standard. As information systems grow in complexity, effective security systems must evolve. With the proliferation of the number of vulnerability points introduced by the use of distributed systems some type of assurance is needed that the systems and network are secure. Intrusion detection systems can provide part of that assurance.

- Operating system, user accounting, and application software audit logging processes must be enabled on all host and server systems.
- Alarm and alert functions of any firewalls and other network perimeter access control systems must be enabled.
- Audit logging of any firewalls and other network perimeter access control system must be enabled.
- Audit logs from the perimeter access control systems must be monitored/reviewed daily by the system administrator.
- System integrity checks of the firewalls and other network perimeter access control systems must be performed on a routine basis.
- Audit logs for servers and hosts on the internal, protected, network must be reviewed on a weekly basis. The system administrator will furnish any audit logs as requested by the ISM.
- Host based intrusion tools will be checked on a routine.
- All trouble reports should be reviewed for symptoms that might indicate intrusive activity.
- All suspected and/or confirmed instances of successful and/or attempted intrusions must be immediately reported according to the Incident Management Standard.

Users shall be trained to report any anomalies in system performance and signs of wrongdoing to the IT Help Desk.

4. Enforcement: Violation of this standard may result in disciplinary action in accordance with El Paso Community College policy and procedures. If you need clarification of this standard, call the Information Security Manager, 831-6312, or contact via e-mail or the IT Help Desk.