UTSA Institutional Compliance
Office of Information Security

OIS 34 – Standard for Threat Detection and Prevention

I. STANDARD STATEMENT

UTSA's Office of Information Security (OIS) is charged with taking steps to preserve the security of the network and devices which are connected to the UTSA network, and is authorized to monitor network traffic and to probe systems, ports and devices for the purpose of identifying attacks and compromises within the network.

II. RATIONALE

This standard supports HOP Policy 8-12 Information Resources Use and Security Policy

III. SCOPE

This standard applies to all UTSA faculty, staff, and students.

IV. CONTACTS

informationsecurity@utsa.edu

V. PROCEDURES

A. All devices connected to the UTSA network are subject to this monitoring, including those not owned and operated by the university.
B. OIS will monitor patterns and attributes of network traffic, but not the information content, except as needed to identify attacks and compromises or at the request of the UTSA legal staff.
C. When potential or confirmed attacks or compromises are detected or threats are identified, OIS may take steps to reduce or eliminate the associated risk. Actions which may be taken include, but are not limited to, blocking access from attack sources, restricting access to targeted UTSA systems, disabling account access, blocking access to vulnerable services and contacting those affected by these actions.

Title: OIS 34 - Standard for Threat Detection and Protection
Effective Date: July 7, 2012
Last Reviewed: August 14, 2020