Effective: *08/08/2022*
Last Revised: *08/08/2022*

Responsible University Administrator:
Assistant Vice President, IT Security Services

Responsible University Office:
Information Technology Services

Policy Contact:
IT Security Services
security@nebraska.edu

ITS-15: Situational Awareness Standard

Standard Contents

1. Purpose

The purpose of the Situational Awareness Standard is to define the organization's requirements for enforcing effective threat intelligence gathering and review practices. This standard serves as a statement of objectives for the protection of information assets against emerging and identified cyber security threats.

2. Scope

This standard shall apply to all The University of Nebraska ("The University") technology assets. Any information not specifically identified as the property of other parties, that is transmitted or stored on Information Systems (including email, messages, and files) shall be considered the property of The University and to which this standard applies. All users (employees, contractors, vendors, or others) of Information Systems are responsible for adhering to this standard.

3. Standard Statement

It is the intention of this standard is to establish a threat intelligence capability throughout The University to help the organization implement security best practices regarding the collection, review, and communication of security threat intelligence to enhance security posture and preparedness. Deviations from the requirements defined herein in the form of exceptions must be approved in advance and in writing by the Chief Information Security Officer ("CISO") as defined in **ITS Policy Exception Standard**. The following subsections outline the Situational Awareness Standard.

4. Situational Awareness Requirements

4.1 Threat Intelligence

4.1.1 Threat Intelligence Feeds

The University must subscribe to industry and threat information provider feeds to gain access to information surrounding emerging and experienced security threats, alerts, advisories, directives, and attacks throughout the industry.

4.1.2 Threat Intelligence Review

Cyber security threat information feeds must be reviewed by University information security staff to identify threats that are relevant and potentially harmful to University assets. If a threat is deemed critical or of high risk, that threat must be communicated to appropriate stakeholders to determine risk treatment and drive program objectives.

4.1.3 Threat Classification

Threat actors and threat methods should be classified depending on their likelihood to impact the organization. Example threat actors include cyber criminals, privileged insiders, nation states, etc. Example threat vectors include accidental misconfiguration, malicious vulnerability exploit, etc. Threats should be classified based on their ability to impact the confidentiality, integrity or availability of University assets of business value (such as data stores or systems supporting critical processes). Threats should be inventoried and regularly reviewed for relevance. The

8. Approvals and Revision History

Approval of this Standard:

	Name	Title	Date
Authored by:	Richard Haugerud	IT CISO	08/08/2022
Approved by:	Bret Blackman	IT CIO	08/08/2022

Revision history of this Standard:

Version	Date	Description
1.0	08/08/2022	Initial Standard Published