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 Governance, Risk and Compliance team, with coordination from the ITS Security Services team, are responsible for maintaining an up-to-date threat inventory.

A threat event is when a threat has the potential to cause harm to an asset (i.e., a cyber criminal attempt to exploit a vulnerability). Controls in place may increase the organization's resilience to various threats.

Threats should be classified according to the following:

Rating	Description
Critical	A given threat event is likely to occur multiple times a year
High	A given threat event is likely to occur in a given year
Medium	A given threat event is likely to occur once every two years
Low	A given threat event is likely to occur once every four years

5. Standards and Procedures

Standards and procedures specific to this policy are to be documented and maintained by the individual affiliates throughout the University system.

6. Compliance

Compliance Measurement
The University of Nebraska Information Security team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions
Any exception to the policy must be documented and formally approved by the CISO. Standard exceptions must describe:

- The nature of the exception
- A reasonable explanation for why the policy exception is required
- Any risks created by the policy exception
- Risk mitigation plan and duration of the exception
- Evidence of approval by the CISO

Non-Compliance
Failure to comply with University IT standards may result in sanctions relating to the individual's use of IT resources or other appropriate sanctions according to policies applicable to University faculty and staff or student conduct.

7. Related Information

The following is a listing of related Policies, Executive Memoranda, Standards, Controls, and Procedures.

NIST 800-53
NIST 800-171
NU Executive Memorandum 16
NU Executive Memorandum 26
NU Executive Memorandum 41
NU Executive Memorandum 42

University-Wide Policies & Guidelines - https://nebraska.edu/offices-policies/policies
ITS-00 Information Technology Definitions and Roles
ITS Knowledge Base - https://uofnebraska.sharepoint.com/sites/NU-ITS/KB

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