Service Provider Management Standard Template

Courtesy of

Nebraska Cybersecurity Network for Education

January 2025

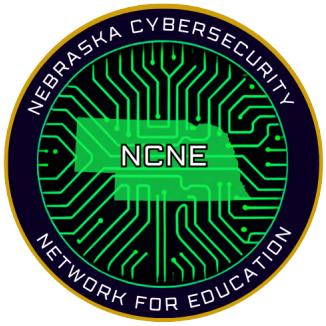

Table of Contents

Service Provider Management Standard Template

Purpose

Commonly referred to as “third-party service providers”, service providers are entities that offer platforms, software, and services to schools. Service providers fulfill necessary business functions but their usage needs to be carefully managed to ensure that data they manage are not exposed to unauthorized third parties. The Service Provider Management Standard provides the processes and procedures for this program.

Responsibility

- The Superintendent of ***<District Name>*** has the primary responsibility for keeping an inventory of the service providers within the enterprise with the caveat of the business unit responsible for contracts and procurement. Before bringing new providers into service, IT must assess that these new providers appropriately fill the enterprise needs while meeting legal and regulatory obligations. Finally, IT must also maintain and decommission all providers. Employees are not empowered to store enterprise data on unauthorized service provider systems.

Exceptions

Exceptions to this standard are likely to occur. Exception requests must be made in writing and must contain:

- The reason for the request,
- Risk to the district of not following the written standard,
- Specific mitigations that will not be implemented,
- Technical and other difficulties in applying patches, and
- Date of review.

Standard

Identify Service Providers

1. At a minimum the inventory of service providers must include:
    a. Name of service provider
    b. Business unit leveraging the platform
    c. Service provider classifications

    d. Point of contact at service provider
    e. Point of contact within the district managing the service provider relationship
2. The service provider inventory must be reviewed and updated annually, or when significant district or service provider changes occur.

Classify Service Providers

1. IT should classify each service provider according to attributes such as:
    a. business function
    b. geographical location
    c. data sensitivity
    d. data volume
    e. availability requirements
    f. applicable regulations
    g. inherent risk or mitigated risk

Assess Service Providers

1. IT should select appropriate and applicable standardized assessment reports, such as Service Organization Control 2 (SOC 2), Payment Card Industry Attestation of Compliance (PCI AoC), customized questionnaires or other appropriately rigorous process, to review service providers against.

Onboarding of Service Providers

1. IT should classify service providers. Classification may use one or more of the characteristics of a service provider. These classifications should be updated and reviewed annually, or when significant district changes occur.
2. IT must ensure service provider contracts include security requirements.

Monitor and Verify Service Providers

1. IT should reassess the service provider to compliance with current assessment requirements annually or more frequently.
2. Additional factors may be monitored, such as release notes and dark web monitoring.

Decommission of Service Providers

1. IT must securely decommission service providers. At a minimum, this includes user and service account deactivation, termination of data flows, and secure disposal of enterprise data within service provider systems.

Revision History

Each time this document is updated, this table should be updated.

Version	Revision Date	Revision Description	Name