8-508. Kiosks and public access workstations.

The purpose of this section is to provide standards and guidelines for kiosks and public access workstations ("kiosks").

(1) Physical Security. (a) All publicly accessible kiosks must be physically secured to prevent theft, tampering, or unauthorized access; (b) kiosks must be installed in well-lit, high-traffic areas to minimize the risk of vandalism, unauthorized access, or tampering; and (c) where feasible, kiosks should be monitored with security cameras.

(2) Access Control. (a) Access to the kiosks' administrative functions and settings must be restricted to authorized personnel only and never granted to the public user; (b) all administrative passwords and access credentials must be securely stored and regularly updated; (c) users should only be granted access to features and functions necessary for their intended use of the kiosk; (d) the kiosks must not be able to access HIGH IMPACT data; and (e) kiosks must be segregated from other state resources by network segmentation or other means.

(3) Software Security. (a) Kiosks must meet the requirements of section 8-504; and (b) access to external devices such as USB and other mass storage devices must be disabled to prevent the introduction of malware or unauthorized software.

(4) Data Protection. (a) Any personally identifiable information ("PII") collected by kiosks must be stored and transmitted using secure protocols; (b) encryption must be used to protect sensitive data both in transit and at rest; and (c) data collected by kiosks must be limited to what is necessary for the intended purpose and must not be retained longer than necessary.

(5) Monitoring and Compliance. (a) Regular audits and monitoring should be conducted to ensure compliance with this policy; and (b) any security incidents or breaches involving kiosks must be promptly reported to the Office of the CIO and investigated.

--

History: Adopted on November 8, 2024.
URL: https://nitc.nebraska.gov/standards/8-508.pdf