

INFORMATION TECHNOLOGY STANDARDS

1. **Introduction.** These Information Technology Standards (these “Standards”) were developed to ensure the security, interoperability, and resiliency of the St. Vrain Valley School District’s (“the District’s”) technology. By ensuring proper cyber hygiene, due diligence is applied to the Contractor’s engagements to prevent and/or minimize the likelihood of adverse events negatively impacting District operations through the loss of availability, capability, technology, and data.

2. **Scope.** These Standards apply to the following:

- a. Storage and/or transmission of District sensitive and/or restricted information;
- b. Storage and/or transmission of District data that is part of the delivery of a District service or capability, such as technology installed directly onto the District on-premises network or cloud-based network infrastructure;
- c. Application integrations that allow data sharing between a District technology asset and a third-party technology asset;
- d. Systems that utilize the District’s network resources including, but not limited to, Wide Area Network (WAN) access, WiFi Network Access, and District Internet Service Provider (ISP) access; and
- e. Managed Service Provider (MSP) contracts, including any engagement requiring the Contractor’s access to any District technology asset.

3. **Minimum Requirements.** The following Minimum Requirements apply to the Contractor’s staff, technology, information systems, services, and applications. During the term of service, the District Technology Services (“DTS”) department may request a written attestation from the Contractor for any of the following minimum requirements. The Contractor shall provide the written attestation within 15 business days of request.

- a. Standards Alignment. These Standards are intended to align with recognized cybersecurity practices, including the NIST Cybersecurity Framework and the CIS Critical Security Controls, where applicable to the District’s technology environment, vendor services, hosted platforms, managed services, and systems that store, process, transmit, or provide access to District data.
- b. Security by Design. Contractors must design, configure, and operate their technology in a manner that supports least privilege, secure authentication, auditability, resiliency, and protection of District data throughout the full lifecycle of the service.

4. **Security.**

- a. Data Security.

- i. *Data Encryption.* All sensitive and/or restricted information must be encrypted using industry-standard encryption protocols in transit, at rest, and during use.
- ii. *Data Retention.* The Contractor must implement a data retention policy that specifies the duration for which data is retained and ensures that data is accessible only for the period necessary to fulfill the service agreement.
- iii. *Data Destruction.* Upon termination of the Contract or at the District's request, all District data must be securely destroyed or deleted per industry-standard practices.
- iv. *Data Segregation.* Data stored or processed must not be commingled with data from other customers. The Contractor must ensure logical or physical separation of the District's data.
- v. *Data Access Controls.* Access to District data must be controlled through robust access management mechanisms, ensuring that only authorized personnel have access based on the principle of least privilege.

b. Account Security.

- i. *Role-Based Access Control ("RBAC").* The Contractor must implement RBAC that ensures system access rights are strictly aligned with an individual's specific job functions and responsibilities. The system must support the principle of least privilege, enabling the configuration of granular access controls limited to the minimum access necessary for required tasks. The solution must provide the capability for the District to regularly audit access rights for necessity and to immediately modify or revoke access upon any change in personnel or responsibilities.
- ii. *Secure Session Management.* The Contractor must ensure that sessions are securely managed and terminated.
- iii. *Multi-Factor Authentication ("MFA") for Local Accounts.* Any application, system, appliance, platform, or service that supports local, native, or non-federated user accounts must support multi-factor authentication for those accounts. This requirement applies to administrative, privileged, support, service management, and standard user accounts where local authentication is used. Local accounts must not be used to bypass District single sign-on, identity governance, conditional access, or MFA requirements. Where Single Sign-on ("SSO") is supported, SSO must be the preferred authentication method unless otherwise approved by the District.
- iv. *Privileged Account Protection.* All administrative, privileged, break-glass, vendor support, and system management accounts must enforce the use

of MFA. Privileged accounts must be uniquely assigned where technically feasible, must not be shared except where explicitly approved by the District, and must be subject to least privilege access controls.

- v. *Account Lifecycle Management.* The Contractor must support timely provisioning, modification, disabling, and removal of user, administrative, vendor, and service accounts. Accounts must be removable or disableable when no longer required. The Contractor must not require continued use of default, shared, or unmanaged accounts except where explicitly approved by the District.
- vi. *Default Accounts and Credentials.* Default credentials must be changed before production use. Default accounts must be disabled, renamed, restricted, or otherwise secured where technically feasible. The Contractor must disclose any default, embedded, shared, vendor support, or manufacturer accounts that cannot be removed or disabled.
- vii. *Authentication and Account Logging.* The Contractor must log authentication events, MFA events, failed login attempts, account creation, account deletion, privilege changes, password resets, and administrative access. Logs must be retained for a minimum period of 90 days and made available to the District upon request for security investigation, audit, or incident response purposes.

c. Patch Management.

- i. *Security Patches.* The Contractor must apply security patches to its systems and applications in a timely manner, following a documented patch management process to address known vulnerabilities.
- ii. *End-of-Life Software Management.* The Contractor must have a process for managing end-of-life software, ensuring that software is updated or replaced before it becomes unsupported and poses a security risk.

d. Information Security Incident Management.

- i. *Incident Reporting Requirements.* The Contractor must establish a communication plan detailing the process for reporting security incidents to the District, including timelines for initial notification and regular updates until resolution.
- ii. *Incident Response Plan.* The Contractor must have a documented incident response plan that outlines procedures for responding to and recovering from security incidents.

e. Remote Access.

- i. *District-Approved Remote Software.* If remote access to the District's network is required, connectivity must be provided through the District-approved Virtual Private Network ("VPN").
 - ii. *MFA Requirements.* Any remote access connections to the District's network must use MFA in the authentication process.
- f. Externally Accessible Systems and Vendor Support Access.
 - i. *Externally Accessible Systems.* Any externally accessible application, administrative interface, vendor portal, management console, or service used to access, process, transmit, or manage District data must support MFA for all user and administrative authentication methods.
 - ii. *Vendor Support Access.* Vendor support access must be disabled by default or restricted to approved support windows where technically feasible. Vendor support access must require MFA, must be logged, and must be limited to the minimum access necessary to perform the approved support activity.

5. Interoperability.

- a. Student Information.
 - i. *EdTech Integration.* Student Demographic/Rostering/Curriculum integration must adhere to 1EdTech Standards unless otherwise agreed upon. More information can be found at <https://www.1edtech.org/standards/details>
 - ii. *EdFi API Compliance.* In the absence of 1EdTech Standard adherence, integration must be compliant with the EdFi API specifications. More information can be found at <https://api.ed-fi.org>
 - iii. *REST API Provision.* If compliance with neither 1EdTech Standards nor EdFi API is possible, Student Information must be provided via a REST API.
 - iv. *SFTP for Flat File Integrations.* Though strongly discouraged, flat file integrations must be conducted via SFTP using modern secure encryption standards.
- b. Employee Information.
 - i. *Teacher Information Rostering.* Teacher information required for rostering purposes must be provided using a 1EdTech interoperability standard, specifically OneRoster. More information can be found at <https://www.imsglobal.org/activity/onerosterlis>

- ii. *Additional Employee Information.* Additional employee information must be accessible via a REST API.
- c. Event Information.
 - i. *Event Notification Interface.* A webhook or similar automation event notification interface is preferred for real-time updates.
 - ii. *Access to Event Information.* If real-time event notifications are unavailable, event information should be accessible via a REST API.

6. Infrastructure and Platform.

a. System Acquisition, Development, and Maintenance (General).

i. *Cloud.*

1. Cloud Platform Provider Preference. Microsoft Azure should be used if a District supplied cloud platform is required to implement the solution.
2. Authentication and Authorization. Applications and services must support District-approved single sign-on using SAML 2.0, OAuth 2.0, OpenID Connect, or another District-approved federated authentication method where available. SSO must be the preferred authentication method for District users. Any local, native, or non-federated account capability must support MFA and must not be used to bypass District identity, access control, conditional access, or MFA requirements.
3. User Group Replication. There must be an ability to replicate user groups from a System for Cross-domain Identity Management ("SCIM") or similar source for consistent access and group management across platforms.
4. Email Authentication. If email is sent on the District's behalf, SPF, DKIM, and DMARC must be supported using the District's email domain, and comply with the District's established DMARC policy.

ii. *Network.*

1. Bandwidth Estimate. The Contractor must provide an estimate of the bandwidth required to support their application or formulas to calculate such usage.
2. Physical Network Access. The Contractor must detail physical network access requirements, including supported IEEE standards.

3. Network Ports Requirements. The Contractor must specify the necessary network ports, distinguishing between TCP and UDP requirements.
4. IP Addressing Requirements. The Contractor must outline their IP addressing needs, including specific configurations or schemes.
5. Internet Access and Public Resource Requirements. The Contractor must describe any requirements for Internet access and their application's use of public resources.

b. On-premise (Operating Systems).

- i. *Microsoft Windows Server.* If a solution requires using Microsoft Windows Server, it must utilize the current build or one revision behind it. The operating system must also be in mainstream support or, at minimum, in the extended support phase with no less than four years remaining.
- ii. *Red Hat Enterprise Linux.* A solution that requires customer-provided Linux must utilize the current build or one revision behind it. Additionally, the operating system must be in full support or, at minimum, in the maintenance support phase with no less than four years remaining.

c. On-premise (Virtualized).

- i. *Virtualized Hardware.* Systems must be compatible with the latest Nutanix AHV build if a solution requires virtualization. Additionally, the virtualized operating system must support the latest Nutanix VirtIO tools for optimal performance, security, and functionality.

7. Artificial Intelligence (“AI”).

a. Generative AI.

- i. *Data Security and Ownership.* The Contractor must not sell or use provided data for further training of AI models without explicit District consent.
- ii. *Reasonable Safeguards.* The Contractor must implement reasonable safeguards to prevent generating inappropriate and/or objectionable content through AI systems.
- iii. *Vendor and Third-Party AI Usage.* The Contractor must ensure that all third-party vendors, sub-processors, or affiliates utilizing AI tools in the provision of services to the District are subject to the same requirements regarding Data Security, Ownership, and Reasonable Safeguards as the Contractor. The Contractor remains responsible and liable for all District

data, including its usage, processing, and protection, by any such third party.

8. Technology Accessibility.

- a. Background. In 2021, the Colorado General Assembly passed HB21-1110 making it a form of discrimination for a state governmental entity to fail to make Information and Communication Technology (“ICT”) accessible to individuals with disabilities. HB21-1110 was codified in Section 24-34-301 et seq., C.R.S.
- b. Applicability. Section 24-34-802(1)(c), C.R.S. specifies that the accessibility standards for individuals with a disability apply to public entities as defined in section 24-34-301(18), C.R.S. Public entities must fully comply with standards established by the Chief Information Officer in the Colorado Office of Information Technology pursuant to section 24-85-103(2.5), C.R.S. The rules apply to all ICT that is in active use on or after July 1, 2024 and any ICT that is newly created, developed, acquired, or purchased on or after July 1, 2024. For ICT not in active use, the rules apply when the ICT is altered or updated, or when an accessible version is requested by an individual with a disability.
- c. Definitions.
 - i. *Accessible or Accessibility.* Accessible or accessibility has the same meaning as defined in section 24-85-102(1.5), C.R.S., or as superseded by a future statute, which is perceivable, operable, and understandable digital content that reasonably enables an individual with a disability to access the same information, engage in the same interactions, and enjoy the same services offered to other individuals, with the same privacy, independence, and ease of use as exists for individuals without a disability.
 - ii. *Information and Communication Technology.* Information technology and other equipment, systems, technologies, or processes, for which the principal function is the creation, manipulation, storage, display, receipt, or transmission of electronic data and information, as well as any associated content. Examples of ICT include, but are not limited to: computers and peripheral equipment; information kiosks and transaction machines; telecommunications equipment; customer premises equipment; multifunction office machines; software; applications; web sites; videos; and, electronic documents. The term does not include any equipment that contains embedded information technology that is used as an integral part of the product, but the principal function of which is not the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. However, if the embedded information technology has an externally available web or computer interface, that interface is considered ICT. For

example, Heating, Ventilation, and Air Conditioning (HVAC) equipment such as thermostats or temperature control devices, and medical equipment where information technology is integral to its operation are not considered information technology.

- d. Technical Standards for Technology Accessibility. The technical standards for technology accessibility for ICT include the following to the extent that they would not require a public entity to take any action that would fundamentally alter the nature of its programs or services, impose an undue burden, or pose a direct threat to the health or safety of others:
 - i. *WCAG.* W3C WCAG 2.1 conformance levels A and AA, as published on Sep. 21, 2023, not including any later amendments or versions, hereby incorporated by reference and available from the Office of Information Technology during regular business hours or at Web Content Accessibility Guidelines (WCAG) 2.1 (W3C).
 - ii. *Hardware.* Hardware that contains a user interface may also need to meet, as applicable, the technical standards contained in US Section 508 of the Rehabilitation Act of 1973 Chapter 4: Hardware, as issued on Jan. 22, 2018, not including any later amendments or versions, hereby incorporated by reference and available from the Office of Information Technology during regular business hours or at About the ICT Accessibility 508 Standards and 255 Guidelines Chapter 4: Hardware (U.S. Access Board).

9. Exception Process. Exceptions for portions of these Standards may be given in written form by the District's Director of Information Security and Systems Architecture. If an exception is requested, please provide a document that describes the need for an exception for each numbered minimum requirement, outlining the need for the exception and specifying each minimum requirement for which an exception is sought.

- a. MFA Exception Requirements. Any exception to MFA requirements must include a documented business or technical justification, the account types affected, the data or systems accessible through those accounts, compensating controls, monitoring capabilities, expected remediation timeline, and explicit written approval from the District's Director of Information Security and Systems Architecture.
- b. Compensating Controls. Requests for exception must identify compensating controls that reduce risk to an acceptable level, including any available logging, network restriction, administrative approval, limited support windows, account monitoring, password rotation, or manual review processes.