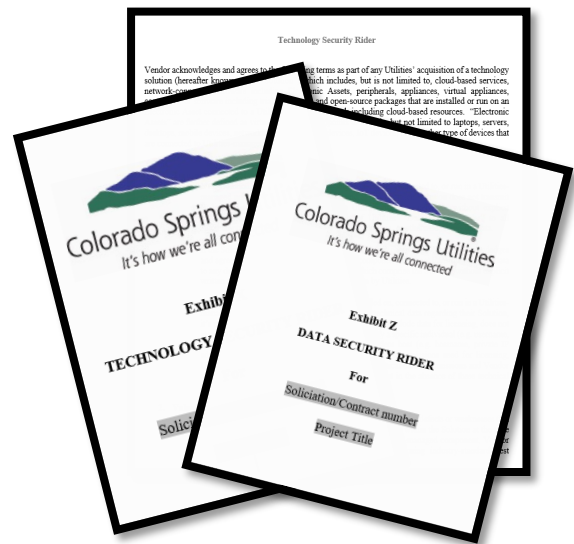


Cybersecurity plays a vital role in protecting the systems and information that support the essential services that our community depends on every day. As important partners in this service delivery, Colorado Springs Utilities maintains risk-based cybersecurity requirements for our suppliers. These requirements help strengthen operational resilience, reduce risk, and support our shared commitment to serving the community safely, reliably, and responsibly.

Are there cybersecurity requirements for all suppliers?

Yes. All suppliers are expected to maintain reasonable cybersecurity practices appropriate to the nature of the products or services they provide.

Requirements may vary based on the scope of work, the sensitivity of information involved, and the level of access granted to organizational systems, facilities, or data. Additional security controls, assessments, or contractual obligations may apply where warranted by risk.



What cybersecurity certifications are required before Colorado Springs Utilities will share sensitive data?

Depending on the nature of the services provided and the sensitivity of the data involved, suppliers may be required to maintain an independently verified cybersecurity certification.

Acceptable certifications include:

- SOC 2 Type 2
- ISO/IEC 27001
- CMMC Level 2 (C3PAO).

Suppliers may also be required to provide evidence of penetration testing and other security documentation as part of the procurement, contracting, or vendor risk review process.

Specific requirements are defined in the applicable contract documents and may vary based on the risk associated with the products, services, or data involved.



Did you know?

Contracts that contain any technology aspects within their scope must go through an internal cybersecurity review to determine the need for any additional cybersecurity requirements.

Must suppliers provide evidence of cybersecurity certifications and penetration testing before a contract can be executed?

Yes. Suppliers that are required to maintain a cybersecurity certification must possess a current certification and have completed applicable penetration testing prior to contract execution.

Before a contract is signed, the supplier must provide an attestation confirming that the required certification is in place and that penetration testing has been performed. The full certification report will be required after contract execution. Specific

findings from penetration tests are not required; only evidence that the testing has occurred from a reputable and certified third party and management commitment to address results.

Why don't I see more cybersecurity-related sourcing events?

Certain cybersecurity-related projects are not publicly advertised due to the sensitive nature of the work and the potential security risks associated with disclosing details about the organization's systems, infrastructure, or security controls.

Who is responsible for the cybersecurity practices of a supplier's subcontractors and other third parties?

The supplier remains responsible for the cybersecurity, confidentiality, and data protection obligations associated with the products and services it provides to Colorado Springs Utilities, including any subcontractors, suppliers, service providers, or other third parties used in the performance of the contract. Suppliers must ensure that such parties comply with applicable contractual, cybersecurity, and data protection requirements. The use of subcontractors or other third parties does not relieve the supplier of its responsibility to protect Utilities' systems, information, or operations.

What authentication methods are required for supplier personnel accessing Utilities systems?

Suppliers whose personnel require access to Colorado Springs Utilities' systems, applications, or data must use multifactor authentication (MFA). At a minimum, Microsoft Authenticator is required to be combined with other methods for interactive user authentication. Authentication requirements may vary based on the sensitivity of the information accessed, the level of access granted, and applicable security requirements.

Will Colorado Springs Utilities provide laptops, mobile phones, tablets, or other equipment to supplier personnel?

No. Suppliers are responsible for providing and maintaining all laptops, workstations, mobile phones, tablets, and other devices used by their personnel to access Utilities systems, applications, or data. Suppliers must implement appropriate security controls to protect these devices, including maintaining supported software, applying security updates, using endpoint protection, and monitoring devices for security events.

Supplier-provided devices used for authentication, including mobile phones used to run Microsoft Authenticator or other approved authentication methods, are subject to the same security expectations. Suppliers are responsible for ensuring that such devices are properly secured, managed, and monitored throughout the period of access.



Did you know?

If required by your contract, you are responsible for providing and updating the necessary reports and/or certificates to Colorado Springs Utilities.

Can suppliers use Colorado Springs Utilities' data to develop, train, or improve artificial intelligence (AI) models?

No. Utilities data may only be used for the purposes authorized by the applicable contract and may not be used to train, improve, or develop AI or machine learning models.



Visit [csu.org](https://www.csu.org) to learn more