CSi a technology integration company

338 Streeter Drive, North Sioux City, SD 57049 | P. 712.255.1775 | F. 712.255.1477

Proposal

Yankton County SD
321 W 3rd Street
Yankton, SD 57078

Provider

CSI, L.L.C.
338 Streeter Drive, North Sioux City, SD 57049

CAGE CODE: 03NA6 / DUNS: 123599362
SPIN: 143050617 / 498 ID: 143054021 / FCC FRN: 0022328405

a technology integration company

338 Streeter Drive, North Sioux City, SD 57049 | P. 712.255.1775 | F. 712.255.1477

Experience

CSI, L.L.C. is an information technology solutions company. We are headquartered in North Sioux City, SD and have been in operation for over 25+ years. We provide Technology Solutions throughout the United States.

CSI, L.L.C. has partnered with some of the top Companies in the Industry.

- Microsoft Gold Partner
- Cisco Partner
- Dell Partner
- SonicWALL – Gold Partner

CAGE CODE: 03NA6 / DUNS: 123599362 / SPIN: 143050617 / 498 ID: 143054021 / FCC FRN# 0022328405

Principal Contact

Nathan Sandage
338 Streeter Drive
McCook Lake, SD 57049
Phone :712-255-1775 x 2105
Fax: 712-255-1477
Email: nsandage@csinov.com

CSI a technology integration company

338 Streeter Drive, North Sioux City, SD 57049 | P. 712.255.1775 | F. 712.255.1477

CSI Managed IT – Pricing:

CSI Total Care Platinum Support	Monthly Total
Includes coverage for the following devices: (5) Fully Managed Server(s) (5) Fully Managed Virtual Server(s) (5) Fully Managed Firewall(s) (15) Fully Managed Network Device(s) (22) Fully Managed Access Point(s) (120) Fully Managed Workstation(s)	**$4235 / month**

Note: CSI Fully Managed Onboarding will be invoiced at $125.00/hour.

CSI IT Management, Cybersecurity Guidance, Strategic Guidance, and Other CIO Duties will be invoiced at $125.00/hour.

CSI a technology integration company

338 Streeter Drive, North Sioux City, SD 57049 | P. 712.255.1775 | F. 712.255.1477

Strategic Future Project Planning

CSI, L.L.C. is aware of Yankton County's upcoming projects over the next 1–3 years and is prepared to support their successful implementation. These initiatives include:

1. **Streamlining Internet Services**
   Consolidating five separate internet services to enhance efficiency, reduce costs, and improve reliability.
2. **Hardware Upgrades & Server Consolidation**
   Upgrading workstations and merging two servers at the Safety Center into a single, more efficient system.
3. **Network Unification at the Safety Center**
   Integrating Safety Center networks to create a more cohesive and effective infrastructure.

Leveraging our broad expertise, CSI, L.L.C. will evaluate various scenarios to ensure optimal solutions for each project.

338 Streeter Drive, North Sioux City, SD 57049 | P. 712.255.1775 | F. 712.255.1477

CSI, L.L.C. References:

John Mangalindan
Administrator - Heartland Center for Reproductive Medicine
832-421-1762
jmangalindan@heartlandfertility.com

Rod Bradley
Retired Chief of Police - Denison Police Department
712-267-3269
Rbradley@denisonpd.net

Cindy Harpenau
Executive Director – Mid-Sioux Opportunity, Inc.
712-786-3420
charpenau@midsioux.org

Sheila Vondrak, RN BSN
Administrator - Siouxland Women's Healthcare
712-252-3044
sheilav@siouxlandwomenshealth.com

Michael Archuleta
CIO - Mount San Rafael Hospital and Clinics
Office: 719-846-8029
marchuleta@msrhc.org

Lon Knievel
CEO - Osmond General Hospital and Clinics
402-748-3393
lknievel@oghne.com

Yankton County reserves the right to terminate this solicitation prior to entering into any agreement with any qualified firm pursuant to this Request for Proposal, and by responding hereto, no firms are vested with any rights in any way whatsoever.

Yankton County reserves the right to reject any or all proposals for not complying with the terms of this RFP.

RFP/RFQ RESPONSE CERTIFICATION COVER FORM

Instruction: To fulfill your RFP/RFQ response, this form must be completed, printed, signed, and included with your submission.

SECTION 1 - RESPONDENT INFORMATION

RFP/RFQ Number: RFP 2025-1

RFP/RFQ Title: Information Technology (IT) Services

RFP/RFQ Respondent Name: CSI, L.L.C.

Address: 338 Streeter Drive
McCook Lake, SD 57049

Telephone: 712-255-1775

Fax: 712-255-1477

Contact Name: Nathan Sandage

Contact Title: Solutions Consultant

Contact Email: NSandage@csinow.com

SECTION 2 —DISCLOSURES

RFP/RFQ Respondents must respond to every statement. RFP/RFQ Responses submitted without a complete response may be deemed nonresponsive.

Indicate "Y" (Yes) or "N" (No) for Disclosures 1-4, and if "Yes," provide details below.

N 1. State whether the Respondent, or any officer, director, manager, stockholder, member, partner, or other owner or principal of the Respondent or any parent, subsidiary, or affiliate has been subject to suspension or debarment by any federal, state, or municipal governmental authority, or the subject of criminal prosecution, or convicted of a criminal offense within the previous 5 years. If "Yes," provide details below.

N 2. State whether the Respondent, or any officer, director, manager, stockholder, member, partner, or other owner or principal of the Respondent or any parent, subsidiary, or affiliate has had any contracts with a federal, state, or municipal governmental authority terminated for any reason within the previous 5 years. If "Yes," provide details below.

N 3. State whether the Respondent, or any officer, director, manager, stockholder, member, partner, or other owner or principal of the Respondent or any parent, subsidiary, or affiliate has been fined more than $5000 for violation(s) of any Rhode Island environmental law(s) by the Rhode Island Department of Environmental Management within the previous 5 years. If "Yes," provide details below.

N 4. State whether any officer, director, manager, stockholder, member, partner, or other owner or principal of the Respondent is serving or has served within the past two calendar years as either an appointed or elected official of Yankton County, including without limitation, any entity created as a legislative body or public or state agency by the general assembly or constitution of this state.

Disclosure details (continue on additional sheets if necessary):

SECTION 3 —OWNERSHIP DISCLOSURE

Respondents must provide all relevant information. Respondent proposals submitted without a complete response may be deemed nonresponsive.

If the Respondent is publicly held, the Respondent may provide owner information about only those stockholders, members, partners, or other owners that hold at least 10% of the record or beneficial equity interests of the Respondent; otherwise, complete ownership disclosure is required.

List each officer, director, manager, stockholder, member, partner, or other owner or principle of the Respondent, and each intermediate parent company and the ultimate parent company of the Respondent. For each individual, provide his or her name, business address, principal occupation, position with the Respondent, and the percentage of ownership, if any, he, or she holds in the Respondent, and each intermediate parent company and the ultimate parent company of the Respondent.

SECTION 4 —CERTIFICATIONS

Respondents must respond to every statement. Responses submitted without a complete response may be deemed nonresponsive.

Indicate "Y" (Yes) or "N" (No), and if "No," provide details below.

THE RESPONDENT CERTIFIES THAT:

Y 1. The Respondent will immediately disclose, in writing, to Yankton County any potential conflict of interest which may occur during the term of any contract awarded pursuant to this solicitation.

Y 2. The Respondent possesses all licenses and anyone who will perform any work will possess all licenses required by applicable federal, state, and local law necessary to perform the requirements of any contract awarded pursuant to this solicitation and will maintain all required licenses during the term of any contract awarded pursuant to this solicitation. In the event that any required license shall lapse or be restricted or suspended, the Respondent shall immediately notify Yankton County in writing.

Y 3. The Respondent will maintain all required insurance during the term of any contract pursuant to this solicitation. In the event that any required insurance shall lapse or be canceled, the Respondent will immediately notify Yankton County in writing.

Y 4. The Respondent understands that falsification of any information in its RFP/RFQ response or failure to notify Yankton County of any changes in any disclosures or certifications in this Respondent Certification may be grounds for suspension, debarment, and/or prosecution for fraud.

Y 5. The Respondent has not paid and will not pay any bonus, commission, fee, gratuity, or other remuneration to any employee or official of Yankton County for the purpose of obtaining an award of a contract pursuant to this solicitation. The Respondent further certifies that no bonus, commission, fee, gratuity, or other remuneration has been or will be received from any third party or paid to any third-party contingent on the award of a contract pursuant to this solicitation.

Y 6. This RFP/RFQ response is not a collusive RFP/RFQ response. Neither the Respondent, nor any of its owners, stockholders, members, partners, principals, directors, managers, officers, employees, or agents has in any way colluded, conspired, or agreed, directly or indirectly, with any other Respondent or person to submit a collusive response to the solicitation or to refrain from submitting response to the solicitation, or has in any manner, directly or indirectly, sought by agreement or collusion or other communication with any other Respondent or person to fix the price or prices in the response or the response of any other Respondent, or to fix any overhead, profit, or cost component of the price in the response or the response of any other Respondent, or to secure through any collusion, conspiracy, or unlawful agreement any advantage against Yankton County or any person with an interest in the contract awarded pursuant to this solicitation. The price in the response is fair and proper and is not tainted by any collusion, conspiracy, or unlawful agreement on the part of the Respondent, its owners, stockholders, members, partners, principals, directors, managers, officers, employees, or agents.

Y 7. The Respondent will comply with all of the laws that are incorporated into and/or applicable to any contract with Yankton County.

Certification details (continue on additional sheet if necessary):

Submission by the Respondent of a response pursuant to this solicitation constitutes an offer to contract with Yankton County on the terms and conditions contained in this solicitation and the response. The Respondent certifies that: (1) the Respondent has reviewed this solicitation and agrees to comply with its terms and conditions; (2) the response is based on this solicitation; and (3) the information submitted in the response (including this Respondent Certification Cover Form) is accurate and complete. The Respondent acknowledges that the terms and conditions of this solicitation and the response will be incorporated into any contract awarded to the Respondent pursuant to this solicitation and the response. The person signing below represents, under penalty of perjury, that he or she is fully informed regarding the preparation and contents of this response and has been duly authorized to execute and submit this response on behalf of the Respondent.

RESPONDENT

Date: 5/14/2025

Carl J. Curry
Name of Respondent

Carl J Curry
~~Signature in ink~~

~~Printed name and title of person signing on behalf of Respondent~~

RFP response Cover From:

RFP Number:**2025-1**

RFP Title: **Information Technology (IT) Services**

Respondent Name: Workplace by Direct

2425 S. Shirley Avenue

605-777-1887

Contact Name: Thom DeWald

Contact Title: Industrial Sales Representative

Contact Email: tdewald@workplace-it.com

Workplace BY DIRECT

RFP Response:

Workplace by Direct is honored to submit this proposal to Yankton County for consideration. With a legacy of over 25 years delivering high-quality Managed IT Services to public and private sector organizations, we are confident in our ability to meet the County's current and future technological needs. We respectfully request your consideration and look forward to the opportunity to support Yankton County with trusted, forward-thinking IT leadership.

Founded in 1997, Workplace began with a mission to provide small and mid-sized organizations with reliable, strategic IT support. In 2022, we became part of the Direct family of companies, which includes several specialized service entities—among them, Direct Data Management, a partner referenced throughout this proposal. Being part of Direct has expanded our capabilities while keeping our focus local, accessible, and personal.

Headquartered in Sioux Falls, South Dakota, our entire workforce is based locally. Our team of over 60 full-time professionals all work closely together under one roof, allowing us to communicate efficiently, collaborate effectively, and deliver consistent, high-quality service to every client.

We specialize in delivering comprehensive IT services through a flat-rate model—a predictable, inclusive pricing structure designed to eliminate hourly billing surprises. Our flat-rate plans cover daily support, infrastructure maintenance, cybersecurity protections, end-user training, backup systems, planning services, Camera and door access controls, and more. This model ensures that clients receive proactive, consistent support with no hidden costs.

At Workplace by Direct, we do more than fix issues—we guide strategy, identify risks before they become problems, and build long-term technology roadmaps. Our commitment is to partnership, clarity, and results. We look forward to becoming a strategic extension of your team.

Thank you once again for the opportunity to submit our RFP response—at Workplace by Direct, we take great pride in the services we provide, grounded in our core values of trust, teamwork, financial success, and excellence. We would be happy to present to the committee in person to further explain our approach and answer any questions you may have.

Sincerely,
Joe Henderson
IT Director, Workplace by Direct

The RFP is organized as follows:

Disclosures

Indicate "Y" (Yes) or "N" (No) for Disclosures 1-4, and if "Yes," provide details below.

__N__ 1. State whether the Respondent, or any officer, director, manager, stockholder, member, partner, or other owner or principal of the Respondent or any parent, subsidiary, or affiliate has been subject to suspension or debarment by any federal, state, or municipal governmental authority, or the subject of criminal prosecution, or convicted of a criminal offense within the previous 5 years. If "Yes," provide details below.

__N__ 2. State whether the Respondent, or any officer, director, manager, stockholder, member, partner, or other owner or principal of the Respondent or any parent, subsidiary, or affiliate has had any contracts with a federal, state, or municipal governmental authority terminated for any reason within the previous 5 years. If "Yes," provide details below.

__N__ 3. State whether the Respondent, or any officer, director, manager, stockholder, member, partner, or other owner or principal of the Respondent or any parent, subsidiary, or affiliate has been fined more than $5000 for violation(s) of any Rhode Island environmental law(s) by the Rhode Island Department of Environmental Management within the previous 5 years. If "Yes," provide details below.

__N__ 4. State whether any officer, director, manager, stockholder, member, partner, or other owner or principal of the Respondent is serving or has served within the past two calendar years as either an appointed or elected official of Yankton County, including without limitation, any entity created as a legislative body or public or state agency by the general assembly or constitution of this state.

SECTION 3 —OWNERSHIP DISCLOSURE

Respondents must provide all relevant information. Respondent proposals submitted without a complete response may be deemed nonresponsive.

If the Respondent is publicly held, the Respondent may provide owner information about only those stockholders, members, partners, or other owners that hold at least 10% of the record or beneficial equity interests of the Respondent; otherwise, complete ownership disclosure is required.

List each officer, director, manager, stockholder, member, partner, or other owner or principle of the Respondent, and each intermediate parent company and the ultimate parent company of the Respondent. For each individual, provide his or her name, business address, principal occupation, position with the Respondent, and the percentage of ownership, if any, he, or she holds in the Respondent, and each intermediate parent company and the ultimate parent company of the Respondent.

SECTION 4 —CERTIFICATIONS

Respondents must respond to every statement. Responses submitted without a complete response may be deemed nonresponsive.

Indicate "Y" (Yes) or "N" (No), and if "No," provide details below.

THE RESPONDENT CERTIFIES THAT:

__y__ 1. The Respondent will immediately disclose, in writing, to Yankton County any potential conflict of interest which may occur during the term of any contract awarded pursuant to this solicitation.

__y__ 2. The Respondent possesses all licenses and anyone who will perform any work will possess all licenses required by applicable federal, state, and local law necessary to perform the requirements of any contract awarded pursuant to this

solicitation and will maintain all required licenses during the term of any contract awarded pursuant to this solicitation. In the event that any required license shall lapse or be restricted or suspended, the Respondent shall immediately notify Yankton County in writing.

_y_ 3. The Respondent will maintain all required insurance during the term of any contract pursuant to this solicitation. In the event that any required insurance shall lapse or be canceled, the Respondent will immediately notify Yankton County in writing.

_y_ 4. The Respondent understands that falsification of any information in its RFP/RFQ response or failure to notify Yankton County of any changes in any disclosures or certifications in this Respondent Certification may be grounds for suspension, debarment, and/or prosecution for fraud.

_y_ 5. The Respondent has not paid and will not pay any bonus, commission, fee, gratuity, or other remuneration to any employee or official of Yankton County for the purpose of obtaining an award of a contract pursuant to this solicitation. The Respondent further certifies that no bonus, commission, fee, gratuity, or other remuneration has been or will be received from any third party or paid to any third-party contingent on the award of a contract pursuant to this solicitation.

_y_ 6. This RFP/RFQ response is not a collusive RFP/RFQ response. Neither the Respondent, nor any of its owners, stockholders, members, partners, principals, directors, managers, officers, employees, or agents has in any way colluded, conspired, or agreed, directly or indirectly, with any other Respondent or person to submit a collusive response to the solicitation or to refrain from submitting response to the solicitation, or has in any manner, directly or indirectly, sought by agreement or collusion or other communication with any other Respondent or person to fix the price or prices in the response or the response of any other Respondent, or to fix any overhead, profit, or cost component of the price in the response or the response of any other Respondent, or to secure through any collusion, conspiracy, or unlawful agreement any advantage against Yankton County or any person with an interest in the contract awarded pursuant to this solicitation. The price in the response is fair and proper and is not tainted by any collusion, conspiracy, or unlawful agreement on the part of the Respondent, its owners, stockholders, members, partners, principals, directors, managers, officers, employees, or agents.

_y_ 7. The Respondent will comply with all of the laws that are incorporated into and/or applicable to any contract with Yankton County

Technical Proposal Elements:

1. **Proposed Approach and Work Plan**

Workplace by Direct delivers Managed IT Services through a strategic, flat-rate model centered on proactive support and long-term alignment. We begin each engagement with a thorough, hands-on onboarding process designed to deeply understand the client environment and set the foundation for lasting success.

Workplace assigns a Technical Account Manager to lead this process. This individual becomes the dedicated expert on your organization—guiding onboarding efforts, coordinating with internal teams, and serving as your long-term IT advisor throughout the partnership.

Onboarding & Transition (Weeks 1–6+)

Upon contract execution, our Technical Account Manager (also referred to as a Technical Concierge) leads a structured onboarding approach. This process is divided into three prioritized phases:

- Must-Have Tasks (Weeks 1–3)
    - Finalize contract, establish billing and client points of contact
    - Review existing documentation and conduct full inventory of assets
    - Deploy critical security, monitoring, and management tools
    - Configure administrative access and automated alerting
    - Train our helpdesk and support teams on the County's environment
    - At the completion of this phase, the County will be onboarded and ready for day-to-day IT support through our Helpdesk team.
- Important Tasks (Weeks 4–6)
    - Create detailed network diagrams
    - Launch our internal Network & Security Validation processes
    - Provide end-user orientation and support contact materials
- Nice-to-Have Tasks (Weeks 6–12)
    - Deploy the County's custom Customer Service Dashboard
    - Optimize systems and finalize remaining tool configurations

- Communicate ongoing IT roadmap and set quarterly touchpoints

Ongoing Management (Ongoing)

Following onboarding, our Technical and Non-Technical Account Managers conduct regular strategic meetings with County leadership. We provide budgeting support, lifecycle planning, project guidance, and consistent helpdesk operations under a fixed monthly rate.

It is worth noting that if outdated hardware or unsupported operating systems are identified during onboarding, we will document these risks and present project proposals to bring systems into compliance. This ensures stability, security, and long-term supportability across the County's IT infrastructure.

Timeline of Major Tasks and Milestones

Timeline	Milestone
Weeks 1–3	Contract finalized, documentation gathered, assets inventoried, tools deployed, environment configured — *County becomes Helpdesk-ready*
Week 4	Helpdesk team orientation, alert configuration, network diagramming
Weeks 5–6	End-user onboarding, full operational readiness
Week 7+	Ongoing proactive management, quarterly strategic reviews

2. Primary Point of Contact with Yankton County

During the RFP process the primary point of contact for Yankton County:

Thom Dewald
Technical Sales
Workplace by Direct
tdewlad@workplace-it.com
605-360-0175

Qualifications of the Proposer

Workplace by Direct has been providing managed IT services since 1997, serving over 250 customers across the Midwest and from coast to coast. We support a diverse range of clients including non-profits, city municipalities, law firms, healthcare organizations, industry environments and more, ensuring their IT environments are secure, efficient, and aligned with their business goals.

With a combination of in-house talent and strategic partnerships, including Direct Data Management (an entity of Direct), we offer comprehensive IT services ranging from cybersecurity to data management. Our flat-rate service model delivers reliable, cost-effective IT management to meet the unique needs of our clients, especially in the public sector.

Key roles in our delivery model include:

- Technical Account Managers (TAMs) – Strategic technical leads responsible for long-term IT planning, budgeting, and infrastructure alignment.
- Non-Technical Account Managers (NAMs) – Business-side coordinators focused on communication, outcomes, and client satisfaction.
- Helpdesk Engineers – Certified support professionals delivering responsive, day-to-day technical support.
- Cybersecurity Lead/Team – Specialists responsible for managing risk, threat response, endpoint security, and compliance initiatives.
- Project Infrastructure Managers – Experts overseeing network improvements, hardware refreshes, and deployment timelines.
- Experience & Satisfaction Team – Focused on ensuring smooth service delivery, feedback collection, and continuous improvement.

4. Key Roles Assigned to Yankton County

Workplace by Direct will assign a dedicated team of specialists to support Yankton County. While most individual resources will be finalized upon execution of the agreement and based on availability, the following core roles and structure will be in place, staffed by full-time employees working from our Sioux Falls, South Dakota headquarters:

- **Joe Henderson – IT Director**
  Oversees all strategic and operational functions of Workplace by Direct. Ensures service delivery, alignment with company standards, and executive-level support throughout the partnership.
- **Tyler Meester – Helpdesk Lead**
  Manages all helpdesk operations including staff performance, escalation response, and adherence to Workplace support standards. Ensures smooth day-to-day resolution of County IT issues.
- **Dorin Hemmelman – Cybersecurity Lead**
  Leads cyber security team, the design and enforcement of security best practices. Oversees vulnerability management, threat detection, NIST and CMMC alignment, employee awareness training, and incident response planning.
- **Bill Heinrich – Infrastructure Project Manager**
  Coordinates all infrastructure upgrades and modernization initiatives. Oversees planning, scheduling, vendor coordination, and implementation of network and hardware projects to ensure timely, successful delivery. Coordinates with a project team for execution.
- **Dedicated Technical Account Manager (TAM)** *(TBD)*
  Leads strategic IT planning, hardware lifecycle management, and technical alignment with County needs.
- **Non-Technical Account Manager (NAM)** *(TBD)*
  Provides ongoing business relationship support, aligning IT services with County objectives and coordinating regular review meetings.
- **Helpdesk Support Engineers** *(TBD)*
  Certified CJIS certified, IT support specialists handling desktop support, troubleshooting, and response services, trained in government and compliance-driven environments.

5. Outcome Monitoring and Evaluation Plan

Workplace by Direct deploys a comprehensive suite of monitoring tools across all endpoints and platforms. This enables us to track system health, apply patches, and maintain device compliance. Our security toolset includes antivirus, DNS filtering, and privileged access management to proactively secure the environment.

We provide transparency through a customer-facing dashboard, updated in real time. This includes metrics such as tickets opened and closed, ticket activity by user, workstation patch status, and workstations covered under the support agreement. These tools allow both our team and Yankton County to continuously evaluate service performance and address needs proactively.

Scope of Work Response:

1. **Requirement** CIO / IT Management Services
   i. Strategy - Provide advice and counsel related to technology needs and trends.
      - Cybersecurity
      - Data retention
      - User education / training
      - Collaboration tools
      - Appropriate and effective use of cloud resources.

Workplace Response:

As part of our flat-rate services, Workplace assigns each client a Technical Account Manager and Non-Technical Account Manager to ensure both IT strategy and business needs are aligned. These individuals become your ongoing advisors directly from the onboarding of the account and continue throughout our long-term partnership. They meet with County leadership regularly to review goals, address emerging needs, and adjust direction as necessary.

We provide guidance on cybersecurity, ensuring that your strategies evolve to meet emerging threats and industry best practices. For data retention, we collaborate with your team to establish and maintain compliant policies, leveraging tools such as Microsoft 365 retention and backup solutions. We offer user education and training, ensuring your staff is continuously equipped to

handle cybersecurity and collaborate effectively using tools like Microsoft Teams, SharePoint, and OneDrive. In addition, we advise on the appropriate and effective use of cloud resources, helping you select and implement the best cloud solutions to enhance security, reduce costs, and optimize performance.

ii. IT Governance - Review and provide input to policies and procedures.
- Acceptable internet use
- Use of personal computers and phones
- Email Spam Filtering
- Offsite and on-premises Backups for Disaster Recovery

Workplace Response:

Workplace provides guidance on the development and review of key IT policies, including acceptable internet use, personal device usage, and email security. While policy writing is an add-on service, we help establish guidelines for internet access and site filtering and recommend the use of secure management tools for personal devices. We assist in creating email security policies, such as spam filtering and phishing protection, and offer input on backup and disaster recovery procedures to ensure both on-site and off-site backups are effectively managed.

iii. Cybersecurity guidance and ongoing support
- CMMC knowledge and participation with Registered Practitioner on staff
- Provide proactive guidance on emerging technologies and practices.
- Participate in committees with external parties (government and private sector) as subject matter experts.
- Awareness training
- Cyber insurance renewals
- NIST assessments
- Perform annual penetration tests.
- Perform quarterly password audits. Address emerging trends and techniques to be applied

Workplace Response:

As part of our flat-rate offering, Workplace provides a dedicated cybersecurity team that actively monitors and protects your systems while addressing key security requirements. Our team ensures compliance with CMMC, conducts NIST assessments,

and assists with cyber insurance renewals. We provide cybersecurity awareness training and enforce password requirements with regular forced changes. While penetration testing is not included in our flat-rate proposal, we partner with a trusted provider to offer this service when requested and help manage the testing. By staying ahead of emerging trends and threats, we ensure your organization remains secure and resilient.

iv. Government-specific knowledge

- Manage government Office 365 tenants.
- Assist with responding to federal grants.
- Maintain and support special retention policies for all data.
- Implement email and file search strategies across active tenants and archives for public records discovery.
- IT Infrastructure Evolution - Develop recommendations for hardware and services selection to support improvements (on premise and cloud) Desktops.
- Portable computers
- Printers
- Tablets
- Servers (cloud and/or on premise)
- Networking Equipment
- Provision/maintain integrations between on-site and cloud-based infrastructure.

Workplace Response:

Workplace currently manages several city and county entities and understands the unique retention policies required for compliance. We are familiar with the standard forms and compliance guidelines typically used in these cases. While we are privy to the requirements, we rely on clear compliance guidelines to implement the necessary policies. These can include, but are not limited to, backup data, email retention, internet segregation, and managing restrictions on specific hardware usage throughout the business. We work closely with our clients to ensure all compliance requirements are met and enforced effectively.

V. Identify modern technology for efficiencies, ergonomics, and security.

- Cell Phones
- Email scanning
- Web filtering
- Endpoint protection

Workplace response:

Workplace provides ongoing recommendations for hardware and services, ensuring that the right solutions are selected to support long-term improvements. Our Technical Account Manager acts as a dedicated advisor, helping to choose the best hardware options for your needs, from desktops and servers to networking equipment and portable devices. We also create a Service Replacement Roadmap to ensure that your infrastructure remains current, with no aging technology going unaddressed.

As part of our flat-rate offering, we include essential security tools like email scanning, web filtering, and endpoint protection. These solutions are integrated into your infrastructure, ensuring both on-premise and cloud-based systems are secure and well-maintained for optimal performance.

vi. Strategic Guidance and Project Advising.

- Assist in annual IT budgeting.
- Assist in IT infrastructure planning.
- Planning for office move and/or redesigns.
- New Grant programs
- Design and support for special purpose entities.

Workplace response:

Workplace provides strategic guidance through our Technical Account Managers, who assist with annual IT budgeting and long-term planning as part of our Service Replacement Roadmap plan. Our account managers also maintain regular business-focused touchpoints to ensure IT strategy aligns with organizational objectives. We support and design infrastructure upgrades, all covered under our flat-rate model with no additional labor fees. While we do not proactively pursue grant opportunities, we are happy to assist in completing technical sections of grant applications.

vii. Software Selection and business process advising

i. Accounting integration software
ii. Review of CRM platforms and upgrades
iii. Reporting needs
iv. Project Management software
v. Office 365

Workplace Response:

As part of our management plan, Workplace actively participates in the evaluation and selection of new software, including accounting systems, CRM platforms, and project management tools. We prefer to be involved in any environment changes to ensure alignment with IT strategy and infrastructure. We assist in both advising and implementing software solutions and provide ongoing support where applicable. While we do not serve as functional experts for third-party applications, we manage the technical aspects and recommend maintaining active vendor support plans for all line-of-business software. We also manage Office 365 environments, assist with installations, and provide support for basic functionality across the platform.

2. **Requirement:** Helpdesk Support
   i. Local user Support
      - On-site support at the County's office (minimum to be determined)
      - Provide remote support when not on-site.
      - Workstation troubleshooting, upgrade, and repair
      - Tablet and cell phone troubleshooting and setup.
      - Determining required hardware specifications and ordering hardware and software
      - Installation of new computers, servers, Network equipment, monitors, peripherals
      - Handle intrusions (viruses, spam, malware)
      - Printer Setups maintaining Print Server(s).
      - Perform Onboardings and terminations.

Workplace Response:

Workplace provides comprehensive user support through a combination of remote and on-site services. Most issues are resolved remotely, but we promptly dispatch technicians on-site for critical needs, projects, and upgrades. As part of our flat-rate model, we manage the full hardware lifecycle—including procurement, installation, and scheduled refreshes—through our Service Replacement Roadmap. We also handle workstation, tablet, and phone setup, troubleshooting, and network equipment installations. Our standard security package includes protection from viruses, spam, and malware. Additionally, we manage printer setups, print servers, and fully support employee onboarding and termination workflows.

ii. Infrastructure upkeep / upgrade
    - Physical servers
    - Storage Area Network (SAN)
    - Update Operating Systems (PCs, Macs, and Servers)
    - Update Tablets and Cell Phones Operating Systems
    - Monitoring data backups
    - Monitor and manage WAN/LAN performance & stability (Firewall & Wi-Fi access points)
    - Upgrading firmware on network equipment
    - Physical server room upkeep and support
        - APC Battery backups

Workplace Response:

Workplace fully manages infrastructure upkeep and upgrades as part of our flat-rate service. We support and maintain physical servers, SAN environments, and handle all operating system updates across PCs, Macs, tablets, and phones. Our team actively monitors and manages WAN/LAN performance, including firewalls and Wi-Fi access points, and performs firmware upgrades on all network equipment. We also provide support for server room maintenance and ensure APC battery backups are properly maintained and tested to protect against outages.

iii. Manage Disaster recovery and data retention.
    - Local and cloud backup of servers
    - Perform periodic test restores of server and Microsoft 365 backups.

Workplace Response:

Workplace provides comprehensive local and cloud backup solutions for servers and Microsoft 365 as part of our flat-rate plan. We perform periodic test restores based on client requirements to ensure backup integrity—ranging from simple file recovery tests to more extensive restoration scenarios. Our backup strategy is designed to safeguard critical data and support fast recovery in the event of data loss or disruption.

iv. Training

- Phishing Training/Testing
- Office365, OneDrive, SharePoint, Teams
- Cybersecurity best practices
- AI best practices

Workplace Response:

Workplace provides phishing simulations and user awareness training as part of our flat-rate service. We offer support and basic training for Office 365 applications, including OneDrive, SharePoint, and Teams. Our team also advises on cybersecurity and AI best practices, helping guide responsible use based on each organization's needs—even as AI technologies continue to evolve.

v. License and warranty management

- Office 365
- Adobe Cloud
- Servers
- Server Operating System
- Need to update list.

Workplace Response:

Workplace manages software licensing and hardware warranties for systems such as Office 365, Adobe Cloud, servers, and server operating systems. We track renewals, ensure compliance, and coordinate support as needed—all included in our flat-rate service model to minimize administrative overhead for your team.

3. <u>Servers Warranty Additional Services</u>

1. Perform on demand emergent services when requested and authorized by Yankton County.

Workplace response:

Workplace is equipped to respond rapidly to on-demand and emergent service needs as requested and authorized by Yankton County. These services—such as system outages, security incidents, or urgent infrastructure issues—are considered within the scope of our flat-rate model when they involve systems under our management. As part of that model, we include on-call and after-hours support, ensuring that emergency items are addressed promptly and effectively to minimize disruption and maintain continuity.

2. Phishing Training/Testing

Workplace response:

Phishing testing and user awareness training are included as part of Workplace's standard security package. We deploy regular phishing simulations and provide follow-up guidance to help users identify and avoid social engineering threats, strengthening your organization's overall cybersecurity posture.

3. SSL certificates for websites

Workplace Response:

While Workplace does not directly manage websites, we do handle domain renewals and DNS management as part of our core services. For SSL certificates and website-related needs, we can coordinate with a trusted partner organization to provide support. These services are available upon request but are not included in our flat-rate offering.

i. Software Development

- Manage custom software and integrations.

Workplace Response:

Workplace does not directly develop or manage custom software or application code. These needs typically fall outside the scope of standard IT support. However, we do have a partner entity under our Direct umbrella (Direct Data Management) that can assist with custom development and integration projects. These services are treated as separate engagements and are not included in our flat-rate model.

ii. Project management and implementation

- New Entities
- Special programs/projects
- Website & Digital Marketing provide ad hoc technical support, development, and enhancements for websites.
- Perform Search Engine Optimization tasks.
- Administer and invoice for passthrough products and subscriptions:
    1. Web and email domains
    2. Software/Hardware, and subscriptions for departments
        - LIST

Workplace Response:

Workplace provides project management and implementation support for new entities and special IT initiatives, as long as they fall under our management scope. We work closely with clients to understand the goals and technical requirements of each project, ensuring smooth execution. When the scope and solution are clearly defined and the entity is covered under an existing agreement, these services are included in our flat-rate model.

Workplace does not provide technical support, development, or enhancements for websites as part of our flat-rate services. However, we can connect clients with our partner company, Direct Data Management, who specializes in these services. Similarly, SEO tasks fall outside the scope of our flat-rate offering, but we can facilitate working with partners for these needs. For administering and invoicing passthrough products, Workplace handles DNS renewals and common software subscriptions, managing these services as part of our support.

Understanding of your environment

- 5 locations
  - Planning and Zoning
  - Sheriff's Office
  - Extension Office
  - Emergency Management
  - Highway Department
- Each location are on separate Domains
- They want to reconcile all locations so they are under one domain at some point
- Fortinet and Sonic Wall Firewalls
- 9 Servers at different locations
- 102 Pc's and laptops
- 15 Ipads
- O365
- Cisco AP's and switches, plus others in all locations

Managed IT Service Arrangement Objectives

The core objectives of the proposed arrangement are to:

- Quickly develop a strong mutual understanding of the technology environment, scope of services and support delivery mechanisms through effective on-boarding.

- Provide end users with a responsive, reliable, predictable, and professional support experience via the Workplace "direct-to-technician" IT Help Desk.

- Ensure availability and stability of the network backbone by monitoring all infrastructure 24/7/365, addressing all alerts/exceptions, and performing structured proactive network operations processes.

- Meet a variety of objectives to maintain a secure, stable, and reliable network through a layered approach to:

Prevention – Avoiding downtime and fight attempts by malicious parties to create IT security incidents.	**Restoral** – Return all data and information systems to normal following a downtime, outage, or security incident.
Detection – Identify real or potential IT operational risks and security threats as quickly as possible.	**Response** – Develop, document, and execute the most appropriate internal and external issue response activities when handling a security or network operations issue.
Containment – Minimize the impact of any IT security incident or network downtime or disruption.	

- Establish IT support as a predictable, known, and fixed business expense with certainty and continuity in resource availability.

- Provide effective direction on future systems evolution, investments, and strategy.

IT Management Scope of Services:

The following table provides a detailed list of our scope of services:

Support Segment	Included Items	Excluded Items
Workplace Internal Security and Stability Assurance **Processes**	▪ Daily Active Directory scans to identify known HW/SW vulnerabilities (e.g., default passwords, missing patches, etc.) ▪ Daily indicator of potential compromise scan to identify exceptions / changes that may indicate compromise (e.g., abnormal login activity, rogue software installation, account add/delete activity, new device discovery, etc.) ▪ Daily report of critical / suspicions changes in O365 environment, user account setup, O/S, DNS activity, etc. ▪ Trend XDR Cloud cross-client and cross-platform alerts of suspicious or malicious activity ▪ Receive, resolve, and thoroughly document exceptions via Workplace Security Desk	
Backbone Devices & Connectivity **Management**	▪ 24/7/365 monitoring of critical devices with real-time alerting: ○ Internet Connection ○ Firewalls ○ Switches ○ Wireless equipment ○ Servers ▪ Installation of service packs and patches on all PCs / laptops / surfaces ▪ Add, change, and delete users as necessary – domains & Office 365 ▪ Implement user permissions & access ▪ Reset passwords when needed ▪ Installation of compatible software products ▪ Replace faulty / failed hardware	▪ Software license costs ▪ Software upgrade costs ▪ Hardware replacement costs ▪ Hardware upgrade costs ▪ Application-specific software support (e.g., Custom Databases, Excel user support) ▪ Installation or repair of data cabling ▪ Web site maintenance

Support Segment	Included Items	Excluded Items
	▪ Monitor / support VoIP applications ▪ Monitoring of backup as scheduled ▪ Updating virus signatures ▪ Managing malware containment software ▪ Monitor user licensing ▪ Monitor & report on available disk space / storage utilized on any drives ▪ Monitor & report on processor utilization ▪ Troubleshoot switches as necessary ▪ Respond to any new issues ▪ Assist with evaluating 3rd party products and services ▪ Hardware replacement planning	
End User **Support**	▪ Unlimited end user access to help desk ▪ Structured evaluation, release and installation of service packs and patches on all Windows systems – on-site and remote ▪ Installation of compatible software products ▪ Replace faulty hardware ▪ Updating virus signatures ▪ Administer malware containment products ▪ Installation & configuration of all network equipment & peripherals ▪ Respond to any new issues that may arise ▪ Troubleshooting / resolve printer issues ▪ Troubleshoot / resolve application access issues ▪ Troubleshoot / resolve e-mail issues ▪ 3rd party escalation	▪ Software license costs ▪ Software upgrade costs ▪ Hardware/printer replacement costs ▪ Hardware/printer upgrade costs ▪ Application-specific software support (e.g., Industry Applications, Excel user support) ▪ Any Windows OS prior to Windows 8 ▪ Any Unix device

Support Segment	Included Items	Excluded Items
Product Standardization - Mandatory:	Delivery and persistent administration of: ▪ Trend XDR Anti-virus ▪ Cisco Umbrella Anti-malware ▪ Anti-SPAM Solution (varies based on e-mail environment): ▪ On-site and off-site data backup (varies based on solution) ▪ Firewall management and hardening	
Product Standardization - Optional:	Delivery and persistent administration of: ▪ Perch SIEM/SOC Services ▪ Multi-Factor Authentication	

Workplace BY DIRECT

Flat Rate Management Service Provider Fees & Expenses:

Pricing for our **true flat-rate**, on-going management services is as follows:

Note: The following quote is based on the asset list provided and a brief walkthrough that was conducted. Quantities may be adjusted higher or lower during the onboarding process, as all assets will be fully audited at that time. However, please note that the pricing for the products will remain unchanged; only the quantities will be adjusted accordingly.

One Time Professional Services Fees:

Item	Quantity	Rate	Total	Comments
Professional Services				
One-time On-site Onboarding Fee	1		$7995	Includes travel. This is one time fee
Total One-time Fees – Including On-boarding Services:			$7995	

MAIN OFFICE CORE NETWORK - Monthly Professional Services Fees - Products & Services:

Item	Quantity	Rate	Total	Comments
Backbone Management				
Server Fee-	1	$500	$500	County Bldg- Planning and Zoning
2nd Server Fee	1	$400	$400	
3rd-9th Server fee	7	$200	$1400	
Site Fees	1	$69	$69	Sites without servers will be added to the quantity of this item
Cyber Operations Platform Services (COPS) Fee Tier 2 Client Environment	1	$200	$200	Vulnerability scanning, security monitoring, alert resolution, security patching, advising on security surveys, etc.
Cloud Complexity Management Fee Tier 2 Client Environment	1	$200	$200	Cloud managed applications (office 365/Cloud hosted email/Sharepoint)

Item	Quantity	Rate	Total	Comments
End User Support				
• Unlimited **Dedicated** End User Workstation & Peripheral Support – On-site and Remote	102	$52.75	$5,380.50	Count deemed reliable based on discussions to date. On-boarding will confirm exact number of dedicated PCs. Unlimited access to Workplace Help Desk during and after normal business hours. On-site and off-site / remote assistance.
• Walk up machines	NA	24.25	NA	During onboarding we may deem some of the end points as Walk-ups (Conference rooms, library, non-daily drivers) this are deemed a lower rate.
IPADS	15	$5.49	$82.35	Mobile device managed
Workplace Standard Products				
Knowb4 Training	102	2.50	$255	
Endpoint Protection Suite - Trend Micro XDR Anti-Virus & Cisco Umbrella Anti-Malware	111	$8.80	$976.80	Enhanced package is available which includes SIEM monitoring. We can update at anytime of wanted.
O365 Backup	40	$3	$120	
Company Backups (PCs)	TBD	$9.95	$0	
Advanced Network Monitoring	1	$299	$299	
Server backups	9	$59.95	$539.55	
Off-site data	1000	$.15 per gb	$150	Based on actuals
Total Projected Monthly Recurring *True Flat Rate* Fees:			**$10,572.20**	

Liability Limitation Statement

By signing this agreement, Workplace and Client acknowledge and agree that Workplace's services outlined in this agreement represent Workplace's best practices management program. The terms of this agreement do not create an express or implied warranty with respect to the services provided by Workplace. Client understands and agrees that system downtime, virus infection, business interruption, connection to the public Internet, including but not limited to virus authors, unprotected outside systems, hackers, Internet outages and data loss/corruption, among other risks, are inherent in Client's decision to store and manage its valuable information in electronic form (herein "Inherent Risks"). Clients agree to indemnify and hold Workplace harmless for any damages attributable to such Inherent Risks.

Workplace's obligation is limited to performing proactive system maintenance procedures, which are standard in Workplace's industry, to minimize inherent risks. In no event shall Workplace be liable for any indirect, incidental, special, or consequential damages of any kind or nature whatsoever, including without limitation, loss of profits or other economic loss, arising from or relating to this Agreement or any such Inherent Risks. Workplace's total cumulative liability in connection with this Agreement, whether in contract or tort or otherwise, will not exceed the aggregate amount paid by client to Workplace here under during the twelve (12) month period immediately preceding any such claim.

Assumptions & Important Considerations

This proposal is submitted based on the following assumptions:

- ✓ Arrangement to begin upon completion of the setup scope of work and execution of this document.
- ✓ Optional products and solutions may require further auditing and inventory information of client network. Workplace can provide detailed pricing upon completion of on-boarding activities.
- ✓ Existing staff will work to help secure all access necessary information including administrative ID's and passwords for applications, servers, etc. per our previous outline.
- ✓ On occasion our audit process will reveal existing viruses on workstations or fileservers that can be time-consuming to eliminate. While none is anticipated, any up-front existing virus 'cleanup' work that is required will be billed as time and materials at a rate of $185/hour.
- ✓ Yankton County LLC will designate client liaison, primarily to help prioritize activities.
- ✓ Service Level Expectations:

- ✓ Workplace Help Desk will be staffed from 8:00 a.m. to 5:00 p.m. Any user can call the Workplace Help Desk, providing they have their unique workstation ID.
- ✓ Helpdesk voicemail box will be provided for extended coverage on nights and weekends. Voicemails will designate emergency vs. next business day calls. Workplace commits to a 2-hour response.

✓ Monthly services will be billed in advance, e.g., July Management Fees are billed on June 30th.

✓ This arrangement provides no support for development or maintenance of any Yankton County LLC web sites, application software or other custom-developed software or interfaces. Workplace works with programming businesses locally and can provide recommendations if needed.

✓ Acceptance of this agreement should not be assumed to allow termination of any other existing 3rd party maintenance agreement, for example virus signature subscriptions or Industry Application maintenance fees.

✓ This is to be a 12-month agreement. If not renewed by the end of the 12 months, the contract will proceed on a month-to-month term.

✓ 45 day written notice is required for early termination of this agreement.

✓ Due to licensing increases year to year, agreements are subject to periodic increases.

✓ Products that are annual commitments will need to be fulfilled beyond the termination date.

✓ Exceptions may be if new provider is using same licensing provider

✓ As part of this agreement, Workplace Management provides IT support services and administration to support routine daily business activities. Workplace does not provide, have the tools or training to support or provide computer forensics services that may be part of any litigation activities, digital investigation, or any other computer forensic work. As such, all computer forensic activities are NOT INCLUDED as part of this proposal. We understand that Workplace staff may be required to comment on our normal procedures, activities, and provide information from our documentation systems and will do so as part of this agreement. However, Workplace reserves the right to refuse and/or defer specific requests for assistance with any forensics activity/activities that we are not qualified to perform, or we feel presents risk to our client, unwarranted involvement of our company or in any way potentially jeopardizes the legal proceedings at hand. Client agrees to fully disclose that specific requests are related to current or potential litigation in all cases.

✓ From time to time, we are asked to dispose of retired systems on behalf of our clients. As part of this agreement, Workplace will remove systems from your location and contract with SEAM to properly destroy the hard drive to ensure data is destroyed. We do not provide any logging or reporting related to system destruction as part of this standard disposal process. If compliance or other regulatory obligations require your organization to provide reporting on system destruction or you desire to have full serial number level disposition, we recommend you work directly with SEAM. Disposal charges may apply and are the client's responsibility.

We appreciate your careful consideration of our proposal. We believe that by accepting this proposal you are retaining the highest quality network support professionals

available, in an innovative and cost-effective arrangement. Please feel free to contact me at 605-360-0175 with any questions or email me at tdewald@workplace-it.com.

Regards,

Workplace Management

* * * * * * * * * * *

Proposal Accepted:

Yankton County	Date
Thom DeWald	5/12/2025
Workplace Management	Date

Form **W-9**
(Rev. October 2018)
Department of the Treasury
Internal Revenue Service

Request for Taxpayer Identification Number and Certification

▶ **Go to *www.irs.gov/FormW9* for instructions and the latest information.**

Give Form to the requester. Do not send to the IRS.

Print or type. See Specific Instructions on page 3.

1 Name (as shown on your income tax return). Name is required on this line; do not leave this line blank.

Workplace Technology Center, Inc.

2 Business name/disregarded entity name, if different from above

Workplace IT Management

3 Check appropriate box for federal tax classification of the person whose name is entered on line 1. Check only **one** of the following seven boxes.

☐ Individual/sole proprietor or single-member LLC ☐ C Corporation ☑ S Corporation ☐ Partnership ☐ Trust/estate

☐ Limited liability company. Enter the tax classification (C=C corporation, S=S corporation, P=Partnership) ▶ _____

Note: Check the appropriate box in the line above for the tax classification of the single-member owner. Do not check LLC if the LLC is classified as a single-member LLC that is disregarded from the owner unless the owner of the LLC is another LLC that is **not** disregarded from the owner for U.S. federal tax purposes. Otherwise, a single-member LLC that is disregarded from the owner should check the appropriate box for the tax classification of its owner.

☐ Other (see instructions) ▶

4 Exemptions (codes apply only to certain entities, not individuals; see instructions on page 3):

Exempt payee code (if any) _____

Exemption from FATCA reporting code (if any) _____

(Applies to accounts maintained outside the U.S.)

5 Address (number, street, and apt. or suite no.) See instructions.

2425 S. Shirley Ave. Ste. 101

Requester's name and address (optional)

6 City, state, and ZIP code

Sioux Falls, SD 57106

7 List account number(s) here (optional)

Part I Taxpayer Identification Number (TIN)

Enter your TIN in the appropriate box. The TIN provided must match the name given on line 1 to avoid backup withholding. For individuals, this is generally your social security number (SSN). However, for a resident alien, sole proprietor, or disregarded entity, see the instructions for Part I, later. For other entities, it is your employer identification number (EIN). If you do not have a number, see *How to get a TIN*, later.

Note: If the account is in more than one name, see the instructions for line 1. Also see *What Name and Number To Give the Requester* for guidelines on whose number to enter.

Social security number

Part II Certification

Under penalties of perjury, I certify that:

1. The number shown on this form is my correct taxpayer identification number (or I am waiting for a number to be issued to me); and
2. I am not subject to backup withholding because: (a) I am exempt from backup withholding, or (b) I have not been notified by the Internal Revenue Service (IRS) that I am subject to backup withholding as a result of a failure to report all interest or dividends, or (c) the IRS has notified me that I am no longer subject to backup withholding; and
3. I am a U.S. citizen or other U.S. person (defined below); and
4. The FATCA code(s) entered on this form (if any) indicating that I am exempt from FATCA reporting is correct.

Certification instructions. You must cross out item 2 above if you have been notified by the IRS that you are currently subject to backup withholding because you have failed to report all interest and dividends on your tax return. For real estate transactions, item 2 does not apply. For mortgage interest paid, acquisition or abandonment of secured property, cancellation of debt, contributions to an individual retirement arrangement (IRA), and generally, payments other than interest and dividends, you are not required to sign the certification, but you must provide your correct TIN. See the instructions for Part II, later.

Sign Here Signature of U.S. person ▶ *Noah Stoeckman* Date ▶ *09/12/2023*

General Instructions

Section references are to the Internal Revenue Code unless otherwise noted.

Future developments. For the latest information about developments related to Form W-9 and its instructions, such as legislation enacted after they were published, go to *www.irs.gov/FormW9*.

Purpose of Form

An individual or entity (Form W-9 requester) who is required to file an information return with the IRS must obtain your correct taxpayer identification number (TIN) which may be your social security number (SSN), individual taxpayer identification number (ITIN), adoption taxpayer identification number (ATIN), or employer identification number (EIN), to report on an information return the amount paid to you, or other amount reportable on an information return. Examples of information returns include, but are not limited to, the following.

- Form 1099-INT (interest earned or paid)
- Form 1099-DIV (dividends, including those from stocks or mutual funds)
- Form 1099-MISC (various types of income, prizes, awards, or gross proceeds)
- Form 1099-B (stock or mutual fund sales and certain other transactions by brokers)
- Form 1099-S (proceeds from real estate transactions)
- Form 1099-K (merchant card and third party network transactions)
- Form 1098 (home mortgage interest), 1098-E (student loan interest), 1098-T (tuition)
- Form 1099-C (canceled debt)
- Form 1099-A (acquisition or abandonment of secured property)

Use Form W-9 only if you are a U.S. person (including a resident alien), to provide your correct TIN.

If you do not return Form W-9 to the requester with a TIN, you might be subject to backup withholding. See What is backup withholding, *later.*

By signing the filled-out form, you:

1. Certify that the TIN you are giving is correct (or you are waiting for a number to be issued),

2. Certify that you are not subject to backup withholding, or

3. Claim exemption from backup withholding if you are a U.S. exempt payee. If applicable, you are also certifying that as a U.S. person, your allocable share of any partnership income from a U.S. trade or business is not subject to the withholding tax on foreign partners' share of effectively connected income, and

4. Certify that FATCA code(s) entered on this form (if any) indicating that you are exempt from the FATCA reporting, is correct. See *What is FATCA reporting,* later, for further information.

Note: If you are a U.S. person and a requester gives you a form other than Form W-9 to request your TIN, you must use the requester's form if it is substantially similar to this Form W-9.

Definition of a U.S. person. For federal tax purposes, you are considered a U.S. person if you are:

- An individual who is a U.S. citizen or U.S. resident alien;
- A partnership, corporation, company, or association created or organized in the United States or under the laws of the United States;
- An estate (other than a foreign estate); or
- A domestic trust (as defined in Regulations section 301.7701-7).

Special rules for partnerships. Partnerships that conduct a trade or business in the United States are generally required to pay a withholding tax under section 1446 on any foreign partners' share of effectively connected taxable income from such business. Further, in certain cases where a Form W-9 has not been received, the rules under section 1446 require a partnership to presume that a partner is a foreign person, and pay the section 1446 withholding tax. Therefore, if you are a U.S. person that is a partner in a partnership conducting a trade or business in the United States, provide Form W-9 to the partnership to establish your U.S. status and avoid section 1446 withholding on your share of partnership income.

In the cases below, the following person must give Form W-9 to the partnership for purposes of establishing its U.S. status and avoiding withholding on its allocable share of net income from the partnership conducting a trade or business in the United States.

- In the case of a disregarded entity with a U.S. owner, the U.S. owner of the disregarded entity and not the entity;
- In the case of a grantor trust with a U.S. grantor or other U.S. owner, generally, the U.S. grantor or other U.S. owner of the grantor trust and not the trust; and
- In the case of a U.S. trust (other than a grantor trust), the U.S. trust (other than a grantor trust) and not the beneficiaries of the trust.

Foreign person. If you are a foreign person or the U.S. branch of a foreign bank that has elected to be treated as a U.S. person, do not use Form W-9. Instead, use the appropriate Form W-8 or Form 8233 (see Pub. 515, Withholding of Tax on Nonresident Aliens and Foreign Entities).

Nonresident alien who becomes a resident alien. Generally, only a nonresident alien individual may use the terms of a tax treaty to reduce or eliminate U.S. tax on certain types of income. However, most tax treaties contain a provision known as a "saving clause." Exceptions specified in the saving clause may permit an exemption from tax to continue for certain types of income even after the payee has otherwise become a U.S. resident alien for tax purposes.

If you are a U.S. resident alien who is relying on an exception contained in the saving clause of a tax treaty to claim an exemption from U.S. tax on certain types of income, you must attach a statement to Form W-9 that specifies the following five items.

1. The treaty country. Generally, this must be the same treaty under which you claimed exemption from tax as a nonresident alien.

2. The treaty article addressing the income.

3. The article number (or location) in the tax treaty that contains the saving clause and its exceptions.

4. The type and amount of income that qualifies for the exemption from tax.

5. Sufficient facts to justify the exemption from tax under the terms of the treaty article.

Example. Article 20 of the U.S.-China income tax treaty allows an exemption from tax for scholarship income received by a Chinese student temporarily present in the United States. Under U.S. law, this student will become a resident alien for tax purposes if his or her stay in the United States exceeds 5 calendar years. However, paragraph 2 of the first Protocol to the U.S.-China treaty (dated April 30, 1984) allows the provisions of Article 20 to continue to apply even after the Chinese student becomes a resident alien of the United States. A Chinese student who qualifies for this exception (under paragraph 2 of the first protocol) and is relying on this exception to claim an exemption from tax on his or her scholarship or fellowship income would attach to Form W-9 a statement that includes the information described above to support that exemption.

If you are a nonresident alien or a foreign entity, give the requester the appropriate completed Form W-8 or Form 8233.

Backup Withholding

What is backup withholding? Persons making certain payments to you must under certain conditions withhold and pay to the IRS 24% of such payments. This is called "backup withholding." Payments that may be subject to backup withholding include interest, tax-exempt interest, dividends, broker and barter exchange transactions, rents, royalties, nonemployee pay, payments made in settlement of payment card and third party network transactions, and certain payments from fishing boat operators. Real estate transactions are not subject to backup withholding.

You will not be subject to backup withholding on payments you receive if you give the requester your correct TIN, make the proper certifications, and report all your taxable interest and dividends on your tax return.

Payments you receive will be subject to backup withholding if:

1. You do not furnish your TIN to the requester,

2. You do not certify your TIN when required (see the instructions for Part II for details),

3. The IRS tells the requester that you furnished an incorrect TIN,

4. The IRS tells you that you are subject to backup withholding because you did not report all your interest and dividends on your tax return (for reportable interest and dividends only), or

5. You do not certify to the requester that you are not subject to backup withholding under 4 above (for reportable interest and dividend accounts opened after 1983 only).

Certain payees and payments are exempt from backup withholding. See *Exempt payee code,* later, and the separate Instructions for the Requester of Form W-9 for more information.

Also see *Special rules for partnerships,* earlier.

What is FATCA Reporting?

The Foreign Account Tax Compliance Act (FATCA) requires a participating foreign financial institution to report all United States account holders that are specified United States persons. Certain payees are exempt from FATCA reporting. See *Exemption from FATCA reporting code,* later, and the Instructions for the Requester of Form W-9 for more information.

Updating Your Information

You must provide updated information to any person to whom you claimed to be an exempt payee if you are no longer an exempt payee and anticipate receiving reportable payments in the future from this person. For example, you may need to provide updated information if you are a C corporation that elects to be an S corporation, or if you no longer are tax exempt. In addition, you must furnish a new Form W-9 if the name or TIN changes for the account; for example, if the grantor of a grantor trust dies.

Penalties

Failure to furnish TIN. If you fail to furnish your correct TIN to a requester, you are subject to a penalty of $50 for each such failure unless your failure is due to reasonable cause and not to willful neglect.

Civil penalty for false information with respect to withholding. If you make a false statement with no reasonable basis that results in no backup withholding, you are subject to a $500 penalty.

Criminal penalty for falsifying information. Willfully falsifying certifications or affirmations may subject you to criminal penalties including fines and/or imprisonment.

Misuse of TINs. If the requester discloses or uses TINs in violation of federal law, the requester may be subject to civil and criminal penalties.

Specific Instructions

Line 1

You must enter one of the following on this line; **do not** leave this line blank. The name should match the name on your tax return.

If this Form W-9 is for a joint account (other than an account maintained by a foreign financial institution (FFI)), list first, and then circle, the name of the person or entity whose number you entered in Part I of Form W-9. If you are providing Form W-9 to an FFI to document a joint account, each holder of the account that is a U.S. person must provide a Form W-9.

a. **Individual.** Generally, enter the name shown on your tax return. If you have changed your last name without informing the Social Security Administration (SSA) of the name change, enter your first name, the last name as shown on your social security card, and your new last name.

Note: ITIN applicant: Enter your individual name as it was entered on your Form W-7 application, line 1a. This should also be the same as the name you entered on the Form 1040/1040A/1040EZ you filed with your application.

b. **Sole proprietor or single-member LLC.** Enter your individual name as shown on your 1040/1040A/1040EZ on line 1. You may enter your business, trade, or "doing business as" (DBA) name on line 2.

c. **Partnership, LLC that is not a single-member LLC, C corporation, or S corporation.** Enter the entity's name as shown on the entity's tax return on line 1 and any business, trade, or DBA name on line 2.

d. **Other entities.** Enter your name as shown on required U.S. federal tax documents on line 1. This name should match the name shown on the charter or other legal document creating the entity. You may enter any business, trade, or DBA name on line 2.

e. **Disregarded entity.** For U.S. federal tax purposes, an entity that is disregarded as an entity separate from its owner is treated as a "disregarded entity." See Regulations section 301.7701-2(c)(2)(iii). Enter the owner's name on line 1. The name of the entity entered on line 1 should never be a disregarded entity. The name on line 1 should be the name shown on the income tax return on which the income should be reported. For example, if a foreign LLC that is treated as a disregarded entity for U.S. federal tax purposes has a single owner that is a U.S. person, the U.S. owner's name is required to be provided on line 1. If the direct owner of the entity is also a disregarded entity, enter the first owner that is not disregarded for federal tax purposes. Enter the disregarded entity's name on line 2, "Business name/disregarded entity name." If the owner of the disregarded entity is a foreign person, the owner must complete an appropriate Form W-8 instead of a Form W-9. This is the case even if the foreign person has a U.S. TIN.

Line 2

If you have a business name, trade name, DBA name, or disregarded entity name, you may enter it on line 2.

Line 3

Check the appropriate box on line 3 for the U.S. federal tax classification of the person whose name is entered on line 1. Check only one box on line 3.

IF the entity/person on line 1 is a(n) . . .	THEN check the box for . . .
• Corporation	Corporation
• Individual • Sole proprietorship, or • Single-member limited liability company (LLC) owned by an individual and disregarded for U.S. federal tax purposes.	Individual/sole proprietor or single-member LLC
• LLC treated as a partnership for U.S. federal tax purposes, • LLC that has filed Form 8832 or 2553 to be taxed as a corporation, or • LLC that is disregarded as an entity separate from its owner but the owner is another LLC that is not disregarded for U.S. federal tax purposes.	Limited liability company and enter the appropriate tax classification. (P= Partnership; C= C corporation; or S= S corporation)
• Partnership	Partnership
• Trust/estate	Trust/estate

Line 4, Exemptions

If you are exempt from backup withholding and/or FATCA reporting, enter in the appropriate space on line 4 any code(s) that may apply to you.

Exempt payee code.

- Generally, individuals (including sole proprietors) are not exempt from backup withholding.
- Except as provided below, corporations are exempt from backup withholding for certain payments, including interest and dividends.
- Corporations are not exempt from backup withholding for payments made in settlement of payment card or third party network transactions.
- Corporations are not exempt from backup withholding with respect to attorneys' fees or gross proceeds paid to attorneys, and corporations that provide medical or health care services are not exempt with respect to payments reportable on Form 1099-MISC.

The following codes identify payees that are exempt from backup withholding. Enter the appropriate code in the space in line 4.

1—An organization exempt from tax under section 501(a), any IRA, or a custodial account under section 403(b)(7) if the account satisfies the requirements of section 401(f)(2)

2—The United States or any of its agencies or instrumentalities

3—A state, the District of Columbia, a U.S. commonwealth or possession, or any of their political subdivisions or instrumentalities

4—A foreign government or any of its political subdivisions, agencies, or instrumentalities

5—A corporation

6—A dealer in securities or commodities required to register in the United States, the District of Columbia, or a U.S. commonwealth or possession

7—A futures commission merchant registered with the Commodity Futures Trading Commission

8—A real estate investment trust

9—An entity registered at all times during the tax year under the Investment Company Act of 1940

10—A common trust fund operated by a bank under section 584(a)

11—A financial institution

12—A middleman known in the investment community as a nominee or custodian

13—A trust exempt from tax under section 664 or described in section 4947

The following chart shows types of payments that may be exempt from backup withholding. The chart applies to the exempt payees listed above, 1 through 13.

IF the payment is for . . .	THEN the payment is exempt for . . .
Interest and dividend payments	All exempt payees except for 7
Broker transactions	Exempt payees 1 through 4 and 6 through 11 and all C corporations. S corporations must not enter an exempt payee code because they are exempt only for sales of noncovered securities acquired prior to 2012.
Barter exchange transactions and patronage dividends	Exempt payees 1 through 4
Payments over $600 required to be reported and direct sales over $5,000[1]	Generally, exempt payees 1 through 5[2]
Payments made in settlement of payment card or third party network transactions	Exempt payees 1 through 4

[1] See Form 1099-MISC, Miscellaneous Income, and its instructions.

[2] However, the following payments made to a corporation and reportable on Form 1099-MISC are not exempt from backup withholding: medical and health care payments, attorneys' fees, gross proceeds paid to an attorney reportable under section 6045(f), and payments for services paid by a federal executive agency.

Exemption from FATCA reporting code. The following codes identify payees that are exempt from reporting under FATCA. These codes apply to persons submitting this form for accounts maintained outside of the United States by certain foreign financial institutions. Therefore, if you are only submitting this form for an account you hold in the United States, you may leave this field blank. Consult with the person requesting this form if you are uncertain if the financial institution is subject to these requirements. A requester may indicate that a code is not required by providing you with a Form W-9 with "Not Applicable" (or any similar indication) written or printed on the line for a FATCA exemption code.

A—An organization exempt from tax under section 501(a) or any individual retirement plan as defined in section 7701(a)(37)

B—The United States or any of its agencies or instrumentalities

C—A state, the District of Columbia, a U.S. commonwealth or possession, or any of their political subdivisions or instrumentalities

D—A corporation the stock of which is regularly traded on one or more established securities markets, as described in Regulations section 1.1472-1(c)(1)(i)

E—A corporation that is a member of the same expanded affiliated group as a corporation described in Regulations section 1.1472-1(c)(1)(i)

F—A dealer in securities, commodities, or derivative financial instruments (including notional principal contracts, futures, forwards, and options) that is registered as such under the laws of the United States or any state

G—A real estate investment trust

H—A regulated investment company as defined in section 851 or an entity registered at all times during the tax year under the Investment Company Act of 1940

I—A common trust fund as defined in section 584(a)

J—A bank as defined in section 581

K—A broker

L—A trust exempt from tax under section 664 or described in section 4947(a)(1)

M—A tax exempt trust under a section 403(b) plan or section 457(g) plan

Note: You may wish to consult with the financial institution requesting this form to determine whether the FATCA code and/or exempt payee code should be completed.

Line 5

Enter your address (number, street, and apartment or suite number). This is where the requester of this Form W-9 will mail your information returns. If this address differs from the one the requester already has on file, write NEW at the top. If a new address is provided, there is still a chance the old address will be used until the payor changes your address in their records.

Line 6

Enter your city, state, and ZIP code.

Part I. Taxpayer Identification Number (TIN)

Enter your TIN in the appropriate box. If you are a resident alien and you do not have and are not eligible to get an SSN, your TIN is your IRS individual taxpayer identification number (ITIN). Enter it in the social security number box. If you do not have an ITIN, see *How to get a TIN* below.

If you are a sole proprietor and you have an EIN, you may enter either your SSN or EIN.

If you are a single-member LLC that is disregarded as an entity separate from its owner, enter the owner's SSN (or EIN, if the owner has one). Do not enter the disregarded entity's EIN. If the LLC is classified as a corporation or partnership, enter the entity's EIN.

Note: See *What Name and Number To Give the Requester,* later, for further clarification of name and TIN combinations.

How to get a TIN. If you do not have a TIN, apply for one immediately. To apply for an SSN, get Form SS-5, Application for a Social Security Card, from your local SSA office or get this form online at *www.SSA.gov*. You may also get this form by calling 1-800-772-1213. Use Form W-7, Application for IRS Individual Taxpayer Identification Number, to apply for an ITIN, or Form SS-4, Application for Employer Identification Number, to apply for an EIN. You can apply for an EIN online by accessing the IRS website at *www.irs.gov/Businesses* and clicking on Employer Identification Number (EIN) under Starting a Business. Go to *www.irs.gov/Forms* to view, download, or print Form W-7 and/or Form SS-4. Or, you can go to *www.irs.gov/OrderForms* to place an order and have Form W-7 and/or SS-4 mailed to you within 10 business days.

If you are asked to complete Form W-9 but do not have a TIN, apply for a TIN and write "Applied For" in the space for the TIN, sign and date the form, and give it to the requester. For interest and dividend payments, and certain payments made with respect to readily tradable instruments, generally you will have 60 days to get a TIN and give it to the requester before you are subject to backup withholding on payments. The 60-day rule does not apply to other types of payments. You will be subject to backup withholding on all such payments until you provide your TIN to the requester.

Note: Entering "Applied For" means that you have already applied for a TIN or that you intend to apply for one soon.

Caution: A disregarded U.S. entity that has a foreign owner must use the appropriate Form W-8.

Part II. Certification

To establish to the withholding agent that you are a U.S. person, or resident alien, sign Form W-9. You may be requested to sign by the withholding agent even if item 1, 4, or 5 below indicates otherwise.

For a joint account, only the person whose TIN is shown in Part I should sign (when required). In the case of a disregarded entity, the person identified on line 1 must sign. Exempt payees, see *Exempt payee code,* earlier.

Signature requirements. Complete the certification as indicated in items 1 through 5 below.

1. Interest, dividend, and barter exchange accounts opened before 1984 and broker accounts considered active during 1983. You must give your correct TIN, but you do not have to sign the certification.

2. Interest, dividend, broker, and barter exchange accounts opened after 1983 and broker accounts considered inactive during 1983. You must sign the certification or backup withholding will apply. If you are subject to backup withholding and you are merely providing your correct TIN to the requester, you must cross out item 2 in the certification before signing the form.

3. Real estate transactions. You must sign the certification. You may cross out item 2 of the certification.

4. Other payments. You must give your correct TIN, but you do not have to sign the certification unless you have been notified that you have previously given an incorrect TIN. "Other payments" include payments made in the course of the requester's trade or business for rents, royalties, goods (other than bills for merchandise), medical and health care services (including payments to corporations), payments to a nonemployee for services, payments made in settlement of payment card and third party network transactions, payments to certain fishing boat crew members and fishermen, and gross proceeds paid to attorneys (including payments to corporations).

5. Mortgage interest paid by you, acquisition or abandonment of secured property, cancellation of debt, qualified tuition program payments (under section 529), ABLE accounts (under section 529A), IRA, Coverdell ESA, Archer MSA or HSA contributions or distributions, and pension distributions. You must give your correct TIN, but you do not have to sign the certification.

What Name and Number To Give the Requester

For this type of account:	Give name and SSN of:
1. Individual	The individual
2. Two or more individuals (joint account) other than an account maintained by an FFI	The actual owner of the account or, if combined funds, the first individual on the account[1]
3. Two or more U.S. persons (joint account maintained by an FFI)	Each holder of the account
4. Custodial account of a minor (Uniform Gift to Minors Act)	The minor[2]
5. a. The usual revocable savings trust (grantor is also trustee)	The grantor-trustee[1]
b. So-called trust account that is not a legal or valid trust under state law	The actual owner[1]
6. Sole proprietorship or disregarded entity owned by an individual	The owner[3]
7. Grantor trust filing under Optional Form 1099 Filing Method 1 (see Regulations section 1.671-4(b)(2)(i)(A))	The grantor*
For this type of account:	**Give name and EIN of:**
8. Disregarded entity not owned by an individual	The owner
9. A valid trust, estate, or pension trust	Legal entity[4]
10. Corporation or LLC electing corporate status on Form 8832 or Form 2553	The corporation
11. Association, club, religious, charitable, educational, or other tax-exempt organization	The organization
12. Partnership or multi-member LLC	The partnership
13. A broker or registered nominee	The broker or nominee
14. Account with the Department of Agriculture in the name of a public entity (such as a state or local government, school district, or prison) that receives agricultural program payments	The public entity
15. Grantor trust filing under the Form 1041 Filing Method or the Optional Form 1099 Filing Method 2 (see Regulations section 1.671-4(b)(2)(i)(B))	The trust

[1] List first and circle the name of the person whose number you furnish. If only one person on a joint account has an SSN, that person's number must be furnished.

[2] Circle the minor's name and furnish the minor's SSN.

[3] You must show your individual name and you may also enter your business or DBA name on the "Business name/disregarded entity" name line. You may use either your SSN or EIN (if you have one), but the IRS encourages you to use your SSN.

[4] List first and circle the name of the trust, estate, or pension trust. (Do not furnish the TIN of the personal representative or trustee unless the legal entity itself is not designated in the account title.) Also see *Special rules for partnerships*, earlier.

***Note:** The grantor also must provide a Form W-9 to trustee of trust.

Note: If no name is circled when more than one name is listed, the number will be considered to be that of the first name listed.

Secure Your Tax Records From Identity Theft

Identity theft occurs when someone uses your personal information such as your name, SSN, or other identifying information, without your permission, to commit fraud or other crimes. An identity thief may use your SSN to get a job or may file a tax return using your SSN to receive a refund.

To reduce your risk:

- Protect your SSN,
- Ensure your employer is protecting your SSN, and
- Be careful when choosing a tax preparer.

If your tax records are affected by identity theft and you receive a notice from the IRS, respond right away to the name and phone number printed on the IRS notice or letter.

If your tax records are not currently affected by identity theft but you think you are at risk due to a lost or stolen purse or wallet, questionable credit card activity or credit report, contact the IRS Identity Theft Hotline at 1-800-908-4490 or submit Form 14039.

For more information, see Pub. 5027, Identity Theft Information for Taxpayers.

Victims of identity theft who are experiencing economic harm or a systemic problem, or are seeking help in resolving tax problems that have not been resolved through normal channels, may be eligible for Taxpayer Advocate Service (TAS) assistance. You can reach TAS by calling the TAS toll-free case intake line at 1-877-777-4778 or TTY/TDD 1-800-829-4059.

Protect yourself from suspicious emails or phishing schemes. Phishing is the creation and use of email and websites designed to mimic legitimate business emails and websites. The most common act is sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

The IRS does not initiate contacts with taxpayers via emails. Also, the IRS does not request personal detailed information through email or ask taxpayers for the PIN numbers, passwords, or similar secret access information for their credit card, bank, or other financial accounts.

If you receive an unsolicited email claiming to be from the IRS, forward this message to *phishing@irs.gov*. You may also report misuse of the IRS name, logo, or other IRS property to the Treasury Inspector General for Tax Administration (TIGTA) at 1-800-366-4484. You can forward suspicious emails to the Federal Trade Commission at *spam@uce.gov* or report them at *www.ftc.gov/complaint*. You can contact the FTC at *www.ftc.gov/idtheft* or 877-IDTHEFT (877-438-4338). If you have been the victim of identity theft, see *www.IdentityTheft.gov* and Pub. 5027.

Visit *www.irs.gov/IdentityTheft* to learn more about identity theft and how to reduce your risk.

Privacy Act Notice

Section 6109 of the Internal Revenue Code requires you to provide your correct TIN to persons (including federal agencies) who are required to file information returns with the IRS to report interest, dividends, or certain other income paid to you; mortgage interest you paid; the acquisition or abandonment of secured property; the cancellation of debt; or contributions you made to an IRA, Archer MSA, or HSA. The person collecting this form uses the information on the form to file information returns with the IRS, reporting the above information. Routine uses of this information include giving it to the Department of Justice for civil and criminal litigation and to cities, states, the District of Columbia, and U.S. commonwealths and possessions for use in administering their laws. The information also may be disclosed to other countries under a treaty, to federal and state agencies to enforce civil and criminal laws, or to federal law enforcement and intelligence agencies to combat terrorism. You must provide your TIN whether or not you are required to file a tax return. Under section 3406, payers must generally withhold a percentage of taxable interest, dividend, and certain other payments to a payee who does not give a TIN to the payer. Certain penalties may also apply for providing false or fraudulent information.

vCISO Proposal

5/15/2025

Cole Kratovil
cole.kratovil@sbscyber.com
+1 605-270-7925

SBS CyberSecurity
www.sbscyber.com
info@sbscyber.com
605.923.8722

SBS CyberSecurity

Let's Connect!

5/15/2025

Jon Anderson
Yankton County
321 West 3rd Street, Suite 100
Yankton, SD 57078

Dear Jon Anderson,

Thank you for giving SBS CyberSecurity (SBS) the opportunity to earn your partnership.

Cybersecurity risk management has emerged as a strategic core competency as technology use has become essential for every business model. Our goal is to help your organization adopt a proactive cybersecurity mindset and build an industry-leading cybersecurity culture that allows you to be prepared for a cyber event, efficiently address changes in the ever-evolving digital world, and perform well on any examination.

SBS has guided organizations in cybersecurity program implementation and risk mitigation since 2004. Working with our experienced, education-focused team enables you to better understand your risk, make more informed security decisions around managing that risk, and identify risk-based budget recommendations.

We understand that trust is earned and relationships are built. Supporting your current needs and future goals by providing the most effective combination of quality service, an expert-level team, and cutting-edge technology is our priority.

Thank you for your consideration,

Cole Kratovil

Cole Kratovil

+1 605-270-7925
cole.kratovil@sbscyber.com

WHO WE ARE

SBS CyberSecurity helps business leaders identify and understand cybersecurity risks to make more informed and proactive business decisions. Since 2004, we have been dedicated to assisting organizations with the implementation of valuable risk management programs and mitigating cybersecurity risks.

Our unique approach is founded on offering a customized level of service based on the size and complexity of each organization, not a one-size-fits-all all system. SBS provides turnkey offerings, including risk management solutions, network security, consulting, auditing, and education tailored to each client's needs, providing a personalized experience from start to finish.

CORE VALUES

Our core values guide every aspect of our organization - from making leadership decisions, to nurturing company culture to building relationships with customers, partners, and employees.

PASSION

We are passionate about our work and show pride, enthusiasm, and dedication in everything we do.

COMPASSION

We are compassionate about the success and well-being of our people and our clients.

INNOVATION

We create innovative products and services that help our clients better understand and manage cybersecurity.

EMPOWERMENT

We create a culture of learning that empowers our people to excel through continuous improvement.

WORKING WITH SBS

BLUEPRINT	Develop a better understanding of how individual components of information security work together with the comprehensive Information Security Program (ISP) Blueprint developed by SBS. The blueprint is designed to help organizations manage risk and make better security decisions.
EXPERIENCE	Work with a trusted company with years of experience working alongside trade associations, as well as federal and state regulators in the financial services industry. Although born in financial services, SBS has assisted organizations in various industries in implementing customized programs that promote risk management and mitigate cybersecurity threats and incidents.
EDUCATION	Be empowered to take security into your own hands with SBS' unique focus on providing quality, industry-specific education to financial institutions.
PROACTIVE SECURITY	Take a step toward a more proactive security mindset. SBS enables leaders to be able to identify and understand how cybersecurity risk impacts their business. This knowledge can transform an organization from having a reactive, compliance-based security mindset to one that embraces a proactive security management program.
RELATIONSHIPS	Form a true partnership with SBS, built on our team's desire to listen to your needs and care about your success.
EXPERT STAFF	Collaborate with a team of the highest qualified consultants, auditors, and network security engineers, many of whom hold specialized security certifications and advanced security degrees.
CUSTOMER SERVICE	Connect with our dedicated customer support team to receive personalized training and support that meets your needs. Beyond that, SBS also believes that quality customer service is the responsibility of each employee.

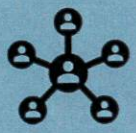
OFFERINGS

RISK MANAGEMENT SOLUTIONS

TRAC™

VERIFY

KNOWBE4



CONSULTING

Cybersecurity Partnership/vCISO

Business Continuity and Incident Response Planning

Vendor Management

Security Awareness Training

Incident Response Team

NETWORK SECURITY TESTING

Network Security Audit

Vulnerability Assessment

Penetration Testing

Social Engineering

AUDIT

IT Audit

Virtual IT Audit

Remote Security Assessment

ACH Audit

Microsoft 365 Controls Assessment

EDUCATION

For a full list of certifications, visit www.sbscyber.com.

ABOUT THE vCISO

Organizations of all shapes and sizes rely heavily on technology, making it almost impossible to do business without it. Managing technology investments, securing confidential information, increasing efficiencies, and embracing a proactive security mindset is crucial, especially when preparing and planning for future success. The strategic first step in evolving your security mindset is appointing a chief information security officer (CISO) dedicated to information security and technology.

Consistent breaches, demand for information security consulting, and a limited supply of qualified specialists all support outsourcing the critical information security officer position as a viable option. With the vCISO service, SBS will provide your organization with a dedicated information security consulting resource to either advise on, assist, or take on many responsibilities of the CISO, including managing the Information Security Program (ISP), governance, risk, and compliance.

A strong ISP must be built on decisions made by each organization. The vCISO agreement is designed to provide expert guidance in making the best decisions to mitigate risk and document customer information and information systems management. Your vCISO will provide your organization with the resources, information, processes, and education to make more informed decisions.

vCISO services are offered at three different levels to meet clients' specific needs. Based on this customer's unique requirements, the Partner level has been selected for this vCISO agreement.

vCISO Partner: SBS will provide an experienced cybersecurity consultant to assist the organization's appointed CISO or ISO in performing their duties. The SBS consultant will work with the organization to create an annual proactive cybersecurity plan to meet the organization's needs and any applicable regulatory requirements. The consultant will share the workload with the CISO/ISO to execute the plan and complete the varying components selected as part of the scope. This level of service is best suited for an organization that has a qualified CISO/ISO, but the individual does not have enough time available to complete all of the items of the organization's information security program.

OPTIONAL ADD-ONS

The following services can be added to a vCISO at an additional cost. If you want more information about a service, please check the box next to its title.

- ☐ Comprehensive network security audit, including:
  - White-box external network penetration test
  - Internal network penetration test
  - Credentialed internal network vulnerability assessment
  - Social engineering – phishing assessment and telephone impersonation
  - Remote access review
  - Firewall configuration review
  - E-mail and spam filtering review
  - Internal network security posture review
- ☐ Full-service vendor management program
- ☐ KnowBe4 phishing email
- ☐ Microsoft 365 implementation review
- ☐ Remote work security assessment
- ☐ Incident Readiness Assessment

VCISO PROPOSAL

Effective Date:

Proposed To:

Yankton County
321 West 3rd Street, Suite 100
Yankton, SD 57078

SBS CyberSecurity, LLC (SBS)
700 S Washington Ave, Ste 200
Madison, SD 57042

605-923-8722
info@sbscyber.com
www.sbscyber.com

QTY	SERVICE/PRODUCT	DESCRIPTION	UNIT PRICE	LINE TOTAL
3	vCISO Partner		$40,200.00	$120,600.00
			TOTAL:	**$120,600.00**

This is a proposal for SBS CyberSecurity, LLC ("SBS" or "Contractor/Licensor") to provide the services described herein ("Services") in exchange for the listed fees plus any applicable travel, meal, and other expenses. This vCISO Proposal ("Proposal") is subject to the terms and conditions in the Services License Agreement ("Agreement"). Upon execution, said Agreement and this incorporated Proposal constitute the entire agreement between the Contractor and Client.

- SBS will invoice the Client upfront annually for the services listed.

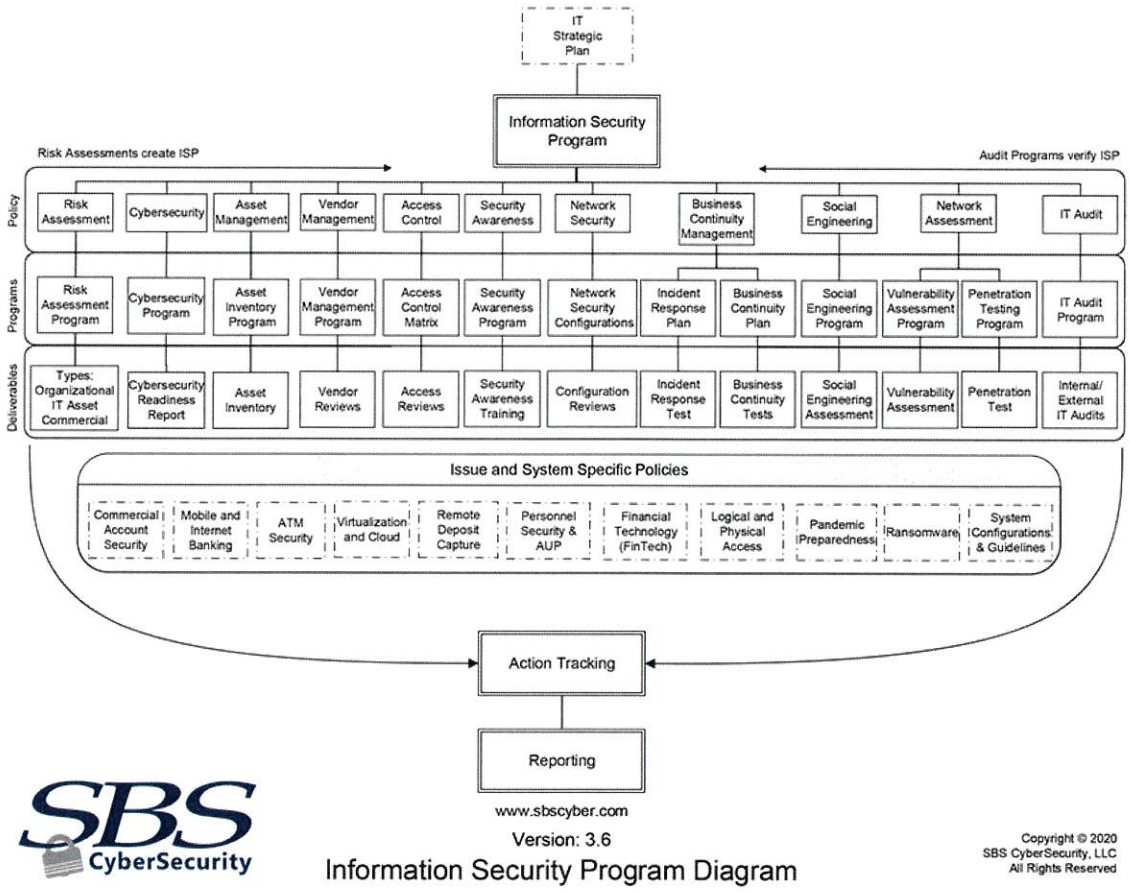
The pricing provided in this Proposal and the availability of SBS resources to complete the "Services" described herein are good for 60 days from 5/15/2025 of this Proposal and are subject to change thereafter.

This Proposal is based on a term of thirty-six (36) months, with the Proposal Effective Date as defined above and with renewals as described in the Agreement.

SBS will not perform additional work beyond the scope of work provided below without prior written consent. Should SBS and Client agree to additional work not described above, such work will be billed at SBS' standard hourly rate.

ISP BLUEPRINT

SBS created the Information Security Program (ISP) Blueprint to depict how a comprehensive, valuable, and repeatable program should flow. The diagram allows our clients to better understand how each component of information security works together. The ISP Blueprint is designed to help the organization confidently manage risk, identify risk-based budget recommendations, and make more informed security decisions.



IN-SCOPE SERVICES

- Information Security Program Annual Workplan Creation and Update
- Cybersecurity Consulting
- Audit/Assessment/Exam Follow-Up
- Cybersecurity News and Updates
- Pre-Recorded Security Awareness Training Videos
- IT Risk Assessment
- Cybersecurity Framework Risk Assessment
- Ransomware Self-Assessment Tool
- ISP Policy/Standards/Procedures Creation and Maintenance
- Business Impact Analysis
- Business Continuity Plan
- Incident Response Plan
- Annual GLBA/ISP Report
- Information Security Program Risk Assessment

OUT-OF-SCOPE SERVICES

- Vendor Management Program Oversight
- Emergency Preparedness Tabletop Exercise Facilitation
- Annual Employee Security Awareness Training
- vCISO Status Reports
- Information Steering Committee Member
- IT Strategic Planning – Cybersecurity Focused
- Security Assessment/ Network Testing Preparation
- Regulatory IT Exam Preparation
- Asset Inventory Management Oversight
- User Access Oversight
- Cybersecurity Insurance Guidance/ Review
- Quarterly Firewall Reviews
- Annual Board/ Sr. Management Education
- Project Planning – Controls Roll-Out
- Incident Response Coordination

SCOPE OF WORK

Executive Summary

SBS CyberSecurity (SBS) has helped many Clients perform activities that support a strong security culture. This Virtual Chief Information Security Officer (vCISO) service provides the Client with a dedicated SBS information security consulting resource. The vCISO and their team will assist an existing CISO or perform many of the functions of a CISO for the Client, depending on the level of service selected.

The vCISO engagement is expected to be performed remotely by the SBS consultant and the SBS team. Onsite visits to the Client's location will be approved by both the Client and SBS where necessary. The Client will be responsible for travel and expenses.

The Client and SBS agree that the responsibility for making Information Security Program-related decisions must remain with the Client, as the Client is ultimately responsible for managing its Information Security Program (ISP). The SBS consultant will participate in all in-scope services according to the work plan and provide the IT steering committee with the resources, information, processes, and education to enable the Client to make the best decisions possible.

As part of the agreement, it may be necessary for the Client to provide training on any software essential for the execution of tasks outlined in this agreement. Both parties agree to cooperate and ensure that adequate training is facilitated to fulfill the obligations outlined herein.

The vCISO service is offered at three (3) various levels of performance from SBS depending on the needs of the Client. The three levels are Guide, Partner, and Pro. A description of what is included for each level is listed with each service. In general, the three levels are:

vCISO Guide: SBS will provide an experienced cybersecurity consultant to guide the Client-appointed CISO or ISO. The SBS consultant will work with the Client to create an annual proactive cybersecurity plan to meet the Client's needs and any applicable regulatory requirements. The consultant will guide the Client through the execution of the plan and the varying components selected as part of the scope. This level of service is best suited for an organization with either an inexperienced CISO/ISO or an organization needing a secondary resource to handle CISO/ISO responsibilities.

vCISO Partner: SBS will provide an experienced cybersecurity consultant to assist the Clients appointed CISO or ISO in performing their duties. The SBS consultant will work with the Client to create an annual proactive cybersecurity plan to meet the Client's needs and any applicable regulatory requirements. The consultant will share the workload with the CISO/ISO to execute the plan and complete the varying components selected as part of the scope. This level of service is best suited for an organization that has a qualified CISO/ISO, but the individual does not have enough time available to complete all of the items of the organization's information security program.

vCISO Pro: SBS will provide an experienced cybersecurity consultant to take on the workload and perform the functions of a CISO or ISO. The SBS consultant will create an annual proactive cybersecurity plan to meet the Client's needs and any applicable regulatory requirements. The consultant will perform the duties of the CISO/ISO to execute the plan and complete the varying components selected as part of the scope. This level of service is best suited for an organization that still needs an appointed CISO/ISO.

Required vCISO Services

Information Security Program Annual Workplan Creation and Update

SBS will create an annual work plan with the Client that includes the tasks and strategic cyber initiatives needed to establish and maintain a proactive ISP and attainable milestones. The work plan will assist SBS and the Client in managing expectations for what processes and services need to happen and when. SBS and the Client will co-manage the ISP progress utilizing this work plan, highlight milestone progress, identify potential gaps, and report shortcomings as needed. Should a milestone's progress become overdue, the work plan will identify the delay and be adjusted to monitor continued progress until completion. At a minimum, the work plan will be reviewed and updated monthly.

Cybersecurity Consulting

A dedicated SBS consultant will be available to advise the Client on cybersecurity issues as needed. Considering our consultant's years of knowledge, clients may experience a reduction in the time and cost of resolving many IT security-related issues. For example, suppose the Client is looking at adding a new technology; the consultant can provide insight into what security risks, mitigating actions, or controls to consider and additional concerns the Client should be aware of before making an informed decision.

Federal regulatory bodies often release new guidance for highly regulated clients that must be included in the Client's information security program. SBS will lead in interpreting this guidance to advise the Client on the steps to ensure appropriate and reasonable compliance. SBS can help save time and money by advising the Client on the proper steps to comply with the new guidance.

Audit/ Assessment/ Exam Follow-Up

Having your information security program assessed by an internal audit resource, a third-party firm, or a regulatory body is a reliable practice, ensuring the program performs efficiently as designed. These assessments often produce "actionable items" or tasks that should be considered to strengthen the program or rectify identified deficiencies. The SBS consultant will review the actionable items for cybersecurity-related issues and discuss options for responding to each item. Plans and milestones to address action items will be developed and included in the ISP work plan and monitored monthly checkpoints as needed.

Cybersecurity News and Updates

SBS will supply the Client with regular communication and information on cybersecurity-related news. This includes access to the SBS "In the Wild" newsletter and links and articles for relevant cybersecurity information. Updates will also be provided as needed for emerging threats the Client should be aware of, including steps that can be taken to mitigate the effects of such threats.

Pre-Recorded Security Awareness Training Videos

SBS consultants produce short training videos to assist Client users in staying current on the relevant cyber threats and trends they need to be aware of. Clients can use these pre-recorded videos to distribute to employees or utilize the videos via a client's learning management system. Video and content requests will be made to the Client's assigned cybersecurity consultant.

In-Scope vCISO Services

SBS has evaluated the needs of the Client and included the following services as in-scope for this engagement.

IT Risk Assessment (TRAC Module available)

The cornerstone of any ISP is a comprehensive IT risk assessment. The IT risk assessment should identify and prioritize the risks associated with the Client's specific use of technology. It will also determine the controls that should be put in place on each technology asset to mitigate risk most effectively. The IT risk assessment evaluates current levels of risk and the controls in place by methodically analyzing each system for risks that may affect how IT systems operate and how that risk affects the Client's overall security.

Partner: SBS and the Client will split the work equally between the SBS consultant and the Client's internal resources and work together to complete the risk assessment.

Cybersecurity Framework Risk Assessment

Whereas the IT risk assessment looks granularly at IT assets, a cybersecurity assessment is a high-level organizational risk assessment that reviews preparedness against cybersecurity attacks. SBS follows the NIST CSF 2.0 framework for evaluating inherent risk and cybersecurity maturity. Alternatively, SBS may utilize a different framework upon request and agreement.

Partner: SBS will go through the risk assessment questions with the Client or split the work equally between the SBS consultant and the Client's internal resource.

Ransomware Self-Assessment Tool

The Ransomware Self-Assessment Tool (R-SAT) provides executive management and the Board of Directors with an overview of an organization's preparedness to identify, protect, detect, respond, and recover from a ransomware attack. The R-SAT is an organizational risk assessment, strategic in nature, that evaluates the risk to your institution from the highest level based on what your institution has and does. The new tool should supplement the Client's tactical risk assessments, whereby the ransomware threat is measured and mitigated.

Partner: SBS will review the tool questions with the Client or split the work equally between the SBS consultant and the Client's internal resource.

ISP Policy/Standards/Procedures Creation and Maintenance (TRAC Module available)

The ISP comprises documents that list and establish the rules and processes the Client will follow regarding information security. Policies establish expectations and rules that guide the Client and are generally approved by the executive level (e.g., Password policy may state that the Client will require complex passwords that are changed frequently). Standards are the methods by which the policy requirements will be implemented. They are generally more flexible, possibly approved by an IT Steering committee (e.g., Password standards documenting specific password length requirements and change frequency). Procedures are detailed step-by-step instructions for completing a task and are approved by a specific department (e.g., step-by-step requirements for implementing password standards on the active directory).

Partner: SBS will split the policies and standards that need to be created/reviewed/updated.

Business Impact Analysis (TRAC Module available)

A Business Impact Analysis (BIA) analyzes a Client's specific processes and their impact on its ability to operate if they are unavailable. The BIA strategically looks at each process's impact on the Client regarding its customers, financial, legal/regulatory requirements, and required recovery resources. The BIA also looks at time frame objectives for recovery, including recovery point objective, recovery time objective, and maximum allowable downtime. This process includes a Business Continuity Risk Assessment, where specific risks affecting business interruptions are evaluated to help the organization identify potential shortfalls in preparedness planning. This information, combined with the interdependency of other business processes, creates a BIA that can help a Client form an effective and efficient strategy to recover from a small or significant business interruption.

Partner: SBS and the Client will split the work equally between the SBS consultant and the Client's internal resources and work together to complete the analysis.

Business Continuity Plan (TRAC Module available)

An essential piece of any Information Security Program is an actionable Business Continuity Plan (BCP). A well-structured BCP will encompass business continuity, disaster recovery, and pandemic preparedness. These plans can help mitigate the unexpected adverse effects of a natural disaster, unplanned power outage, widespread illness, and many other unscheduled events; the BCP will help the Client resume operations as quickly and efficiently as possible. Clients in regulated industries also often need a BCP to demonstrate compliance.

Partner: SBS and Client will split the work equally and work together to complete and update the plan.

Incident Response Plan

Another critical piece of any Information Security Program is an actionable Incident Response Plan (IRP). An IRP is designed to establish a plan to mitigate the adverse effects of a security breach and identify and document triggers of how a Client would know when a security incident may be happening. The incident response plan will outline a decision process from the trigger event to a potential investigation based on various incident types. Not only can an IRP reduce the potential negative severity and consequences of a breach, but it is generally required by most cyber regulations.

Partner: SBS and Client will split the work equally and work together to complete and update the plan.

Annual GLBA/ISP Report

The Gramm-Leach-Bliley Act (the Financial Service Modernization Act) enacted the Financial Privacy Rule and the Safeguards Rule in 1999. The consulting and services proposed in this document are designed to assist the Client in complying with this Act. For non-GLBA regulated Clients, it is still critical to report the "state of the information and cyber security union" to senior management or the Board of Directors at least annually. The top level of the Client must understand that IT, IS, and cybersecurity are not simply an expense but that their business relies on its technology to do business today. Information security is a critical business process, and the board must be kept updated on the risk to the Client and what's being done to mitigate said risk.

Partner: SBS will assist in generating the report and deliver the report to the appropriate party.

Information Security Program Risk Assessment (TRAC Module available)

As technology and risk change, so should your Information Security Program (ISP). An Information Security Program Risk Assessment will identify strengths, weaknesses, and gaps in the current state of the Client's ISP. The risk assessment will help design the road map and work plan to address areas to improve for the most significant risk reduction, assisting the client in measuring progress towards a proactive information security program.

Partner: SBS will go through the risk assessment questions with the Client or split the work equally between the SBS consultant and the Client's internal resource.

Out-of-Scope vCISO Services

Vendor Management Program Oversight (TRAC Module available)

According to various industry regulatory requirements, an organization's board of directors or senior management is ultimately responsible for managing activities conducted through vendor relationships and identifying and managing the risks that arise from these relationships. A Vendor Management Program will help the Client proactively manage the risks of these vendor relationships and meet regulatory requirements. A Vendor Management Program will encompass several components, including risk rating your vendors, establishing and implementing processes for selecting new vendors, regularly gathering and reviewing due diligence documentation from existing vendors, and monitoring vendor contracts to ensure they meet Client risk and performance expectations.

Partner: SBS will offer guidance on establishing, managing, or improving a vendor management program but will not do vendor management.

Emergency Preparedness Tabletop Exercise Facilitation

SBS will facilitate the testing of emergency preparedness plans, including the Business Continuity Plan and the Incident Response Plan, annually by scheduling an approximately half-day to full-day test. The SBS consultant will provide a mock scenario of an event that might happen; the Client will then follow their Plan and take the appropriate steps. SBS will review the results with the Client and recommend proper plan changes to remediate any identified deficiencies.

Partner: SBS will schedule and facilitate the testing annually. SBS will provide feedback and recommendations for plan changes as appropriate.

Annual Employee Security Awareness Training

Security awareness training covering basic information security principles and response steps to social engineering and phishing - the two most common causes of data loss and breaches – is a pillar of a strong cybersecurity culture. Training lowers the risk of falling victim to today's attack methods and helps the Client comply with laws and regulations. Remember that information security is the responsibility of everyone at the Client, not just an individual or committee. An SBS consultant will lead a training program covering topics such as an overview of threats, passwords, social media, acceptable use, Information Security Program, and incident response.

Partner: SBS will schedule, create, and facilitate the training annually.

vCISO Status Reports (Quarterly/ Monthly)

The assigned SBS consultant will have regularly scheduled communication with the Client via meetings (both virtually and in-person if agreed to), phone conversations, emails, etc. The status reports can provide a summary of these communications for Client management to understand the frequency and general content of the communications. The status reports will also give an overview of recent accomplishments on the information security program and a summary of Items to Note.

Partner: SBS will provide status reports to the Client to provide insight into communication and activities between the assigned SBS consultant and Client.

Information Steering Committee Member (Quarterly/Monthly)

IT Steering Committees can go by a variety of names. Still, the committee aims to discuss and make non-board-level decisions on technology and cybersecurity initiatives. Members of this committee should come from various functions and departments of the Client to ensure buy-in from all sides of the organization. The SBS consultant will be a member of this committee and will be involved specifically in the cybersecurity portions of the meeting.

Partner: The SBS consultant or assigned designee will attend the meetings and present on specific areas such as IT Risk assessment, vulnerability scans, etc.

IT Strategic Planning – Cybersecurity Focused

IT Strategic planning should address the long-term goals of the Client and the allocation of IT resources to achieve them. IT Strategic planning focuses on a three to five-year horizon and helps ensure that the Client's technology plans are consistent and aligned with its business plan. The IT Strategic Plan should address the budget, periodic board reporting, and the status of risk management controls. Executive management must develop a strategic plan and set a budget. The CIO or CTO should then develop the IT strategy supporting the Client's business strategy and ensure it aligns with its risk appetite. The CISO is responsible for meeting those risk appetites and reporting to executive management. Each entity creates and maintains an IT Strategic Plan aligned with the Client's overall strategic plan.

Partner: Provide guidance on the risk of IT Strategic initiatives that support the organization's strategic initiatives. Additionally, SBS will monitor progress and keep the organization on track with these risk initiatives throughout the year.

Security Assessment/ Network Testing Preparation

Having your information security program and network security assessed by a third-party firm is a sound practice to ensure the ISP and network are performing and as secure as expected. To perform these sorts of assessments or tests, the third party will generally need to gather information/documentation and ask questions to understand the Client environment better. While putting together this information is usually not hard, it can be time-consuming and frustrating – especially if the Client and the testing firm's terminology don't align.

Partner: SBS and Client will divide responsibilities in gathering documentation/completing questionnaires, etc., for third-party testing.

Regulatory IT Exam Preparation

In many regulatory environments, specifically banking, federal and/or state regulators complete IT examinations to ensure compliance with regulations. Before beginning these examinations, the examiners must gather information/documentation and ask questions to understand the Client's environment better. There are generally interview and discussion requirements during the examination that the Client needs to be prepared for.

Partner: SBS and Client will divide responsibilities in gathering documentation/completing questionnaires, etc., for regulatory exams.

Asset Inventory Management Oversight

Documentation and a complete understanding of a Client's technology assets are vital to managing your data's security. If an organization doesn't understand what technology they have, it becomes impossible to manage the risk of it. An asset management program allows an organization to inventory and manage its technology assets.

Partner: SBS will offer guidance on establishing, managing, or improving an asset management program but will not do asset management.

User Access Oversight

Users need access to various technology applications and programs to perform their job functions. Managing this access when a user changes roles in the organization, leaves, or is placed on cross-functional teams becomes a challenge to ensure they still have proper access, but unneeded access is disabled. Different technology applications also provide varying levels of access controls to ensure users can only make appropriate changes for their job functions. A user access program is a way to manage this access and ensure employees only have access to what they need to protect themselves and the organization better.

Partner: SBS will offer guidance and provide templates on establishing, managing, or improving a user access management program but will not complete user access reviews.

Cybersecurity Insurance Guidance/ Review

Cybersecurity insurance is a tool that an organization can use to mitigate some financial risks of a breach. Cybersecurity insurance policies can be complex and have exceptions for several incidents. SBS can help the Client better understand what their current or potential policy does and does not include and ensure they are aware of those things before they file any possible claims.

Partner: SBS will offer guidance and/or review Clients' Cybersecurity insurance coverage.

Quarterly Firewall Reviews

Firewalls are a primary mechanism to configure and understand the traffic flowing into and out of your network. Regularly reviewing your firewall's configuration, rules, and changes is an excellent proactive cybersecurity move and requires some cybersecurity standards. The firewall review should review existing firewall change management procedures, changes in firewall rules, verification that existing rules are adequate, understanding why specific IPs are allowed, reviewing open ports, etc.

Partner: SBS will provide documentation and training on how to conduct a firewall review. The SBS consultant will complete one full firewall review annually and make appropriate recommendations. The client will be responsible for quarterly change reviews.

Annual Board/Sr. Management Education

Clients must ensure that leadership understands the definition and importance of security awareness and information security. SBS will conduct information security training for the board of directors and other senior management levels to help ensure a culture of cybersecurity. This training program will include information on effectively managing and overseeing information security in an organization. The training will also highlight the organizational controls for cybersecurity and potential cyber weaknesses.

Partner: SBS will annually schedule and facilitate the training.

Project Planning – Controls Roll-Out

Implementing cybersecurity controls and solutions is sometimes the job function of the CISO or ISO. SBS can help create, implement, and/or manage these projects to ensure all aspects are considered and the project is completed.

Partner: SBS will work with the Client to evenly divide the responsibilities of cybersecurity projects to completion.

Incident Response Coordination

An incident coordinator manages the response to an information security incident. This includes identifying and prioritizing security-related incidents, defining appropriate responses, and establishing incident reporting requirements. The incident coordinator works closely with the Information Security Officer (if applicable) to determine the severity of a suspected event and whether full Incident Response Plan activation is necessary. They also coordinate with Incident Response Team Members to gather information, preserve evidence, and provide additional resources as needed throughout the investigation. The incident coordinator ensures that incidents are managed in compliance with existing policies and procedures and may invoke the Business Continuity Plan if the incident impacts the organization's business functions. They are also responsible for compiling proper reporting and organizing lessons learned.

IMPORTANT NOTES:

- SBS does not guarantee specific response times if this service is needed. In the event your assigned SBS resource is unavailable, SBS will make efforts to quickly assign an alternative resource for the purposes of this service.
- Any time used for this service will be invoiced to the Client hourly in addition to the vCISO contract value. The hourly rate will be the current SBS standard hourly rate.
- SBS does not provide active incident response services or digital forensics services. SBS will assist with the incident response coordinator role only. If active incident response or digital forensics services are needed SBS can provide partner recommendations and continue to assist the Client with the incident response coordination.

Partner: SBS will assist the client with incident coordination in the event it is needed during the engagement.

LICENSE AGREEMENT

SERVICES LICENSE AGREEMENT TERMS AND CONDITIONS

The following Terms and Conditions ("Terms") will govern the Services provided by SBS as described in the attached Proposal executed by the Client ("Services"). The Terms and attached Proposal together constitute a single agreement ("Agreement").

1. SERVICES AND PAYMENT

1.1 All Services performed by SBS prior to Client signing this Agreement will be deemed accepted by Client and governed by this Agreement. Changes to this Agreement must be in writing.

1.2 Client will pay SBS the fees for Services shown in the attached Proposal, plus all applicable sales, use or other taxes upon the Services.

1.3 Client will pay SBS for all reasonable expenses incurred in connection with the Services, including out-of-town travel and meal expenses and/or other expenses associated with meetings or presentations requested by Client, whether or not estimated in the Proposal.

1.4 All invoices issued by SBS CyberSecurity are payable within **30 days** from the date of the invoice. If payment is not received within **30 days**, a reminder will be sent. After **60 days** from the invoice date, any outstanding amounts will be subject to an interest charge at the rate of **1.5% per month**, compounded monthly, and a late fee of **$25** or the maximum allowed by applicable law, whichever is less. We encourage our clients to adhere to these terms to avoid any additional charges. Client will be responsible for all collection expenses or attorneys' fees necessitated by a failure to make timely payment.

1.5 In the event Client terminates this Agreement without cause, SBS will invoice Client and Client is obligated to pay for (i) all expenses incurred to the date of termination and (ii) all remaining service fees for the remaining term of the Agreement as described in Section 2.1.

1.6 In the event Client reschedules a service without at least 2 weeks' notice to SBS, a rescheduling fee of $1,000 may be applied to client.

2. TERM AND TERMINATION

2.1 Unless sooner terminated as provided in these Terms, the term of this Agreement will extend to and terminate thirty-six (36) months from the effective date of this Agreement.

2.2 Subject to Client's continuing obligations under Section 1.5, either party may cancel the Agreement at any time, with or without cause, upon 15 days' prior written notice to the other party.

2.3 Upon termination or cancellation of this Agreement for any reason, and per a written request, each party will return all Confidential Information (defined below) to the disclosing party, except as otherwise provided in this Agreement. Termination will not relieve Client's obligation to make payments for Services described in the Proposal and expenses incurred as provided in this Agreement, nor will it limit either party from pursuing other remedies available to it, including injunctive relief.

3. ACKNOWLEDGMENT, WARRANTY AND DISCLAIMERS

3.1 Client acknowledges and agrees that scanning of IP addresses and/or domain names in connection with performance of the Services, may, in some circumstances, result in the disruption of access to Client's site(s). Consequently, Client agrees that it is Client's responsibility to perform backups of data on all devices connected to Client's IP addresses and/or domain names prior to SBS' performance of any Service. Client assumes the risk for all damages, losses, and expenses resulting from loss of access to Client's site(s) or failure to backup data.

3. 2 SBS warrants that all Services will be performed in a diligent and competent manner. This is an exclusive warranty. SBS EXPRESSLY DISCLAIMS ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED WITH RESPECT TO ITS SERVICES INCLUDING REPORTS OR DELIVERABLES, INCLUDING ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, ACCURACY AND ORAL OR WRITTEN STATEMENTS NOT IN THESE TERMS.

3.3 ALL THIRD PARTY PRODUCTS OR SERVICES ARE MADE AVAILABLE "AS IS." SBS MAKES NO WARRANTIES, WHETHER EXPRESS OR IMPLIED, RELATED TO THIRD PARTY PRODUCTS OR SERVICES.

3.4 Client must provide written notice to SBS if any Service fails to conform with Section 3.2 within 30 days of completion of a specific Service. Client's sole remedy, and SBS's entire liability, will be for SBS to re-perform the nonconforming Service within a reasonable time.

4. INDEMNIFICATION AND LIMITATION OF LIABILITY

4.1 Subject to Sections 3.1-3.4, 4.3 and 4.4, SBS will indemnify and hold Client, its officers, directors, employees and affiliates harmless from any damage, loss, liability, or expense (including, without limitation,

reasonable attorneys' fees and expenses) arising out of (i) the negligent or intentional acts or omissions of SBS, its employees, agents or contractors; or (ii) any breach of this Agreement by SBS.

4.2 Subject to Sections 4.3 and 4.4, Client will indemnify and hold SBS, its officers, directors, employees and affiliates harmless from any damage, loss, liability, or expense (including, without limitation, reasonable attorneys' fees and expenses) arising out of (i) the negligent or intentional acts or omissions of Client, its employees, agents or contractors; (ii) any breach of this Agreement by Client; or (iii) Client's interpretation or use of a Service or any report or deliverable provided by SBS.

4.3 Except to the extent required by applicable law, neither party will be liable to the other for any matter arising from or in connection with this Agreement for an amount in excess of the amount actually paid by Client to SBS under this Agreement during the most recent 24-month period. In no event will SBS be liable to the customers of Client for any damages alleged to arise or relate to Client's use of the Services or the failure of any Service to achieve a particular standard.

4.4 NEITHER PARTY WILL BE LIABLE TO THE OTHER PARTY OR ANY THIRD PARTY CLAIMING UNDER THE OTHER PARTY FOR PUNITIVE, INDIRECT, SPECIAL, INDCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING WITHOUT LIMITATION LOSS OF PROFITS OR LOST SALES, ARISING FROM OR RELATING TO THIS AGREEMENT, PERFORMANCE OR FAILURE TO PERFORM THE SERVICES.

5. CONFIDENTIALITY

5.1 "Confidential Information" means any information that is competitively sensitive and is not known to the public regarding the respective businesses of the parties. Confidential Information includes, but is not limited to, trade secrets and intellectual property; customer and source information; financial data and business plans; employee information and service-related information. Client acknowledges that the SBS' products, services, processes and intellectual property are Confidential Information. Confidential Information does not include information which (i) is in the public domain at the time of disclosure; (ii) becomes part of the public domain through no fault of the other party; or (iii) is rightfully received by the other party without obligation from a third party who is free to disclose such information.

5.2 Neither party, nor any of their respective officers, directors, employees, or agents will disclose the other party's Confidential Information to any third parties or use any Confidential Information from the other party for any purpose (competitive or otherwise) unrelated to the performance of this Agreement. Each party will limit dissemination of Confidential Information to persons within their business organization who are directly involved in the performance of Services under this Agreement.

5.3 SBS will use nonpublic customer information obtained from Client only for the purpose for which it was provided. SBS will not sell or share any of this information with anyone not involved in providing services for Client.

5.4 Each party will use the same level of care to prevent the disclosure of Confidential Information of the other party that it exercises in protecting its own Confidential Information, and must, in any event take reasonable precautions to prevent the disclosure of Confidential Information to third parties. Further, SBS will ensure administrative, physical and technical security measures that are no less rigorous than accepted industry standard practice are in place to protect all Confidential Information received from Client or generated as a result of this Agreement.

5.5 Reports or deliverables provided to Client by SBS may be used and distributed by Client, its officers, directors, employees, or agents only for Client's internal business purposes. Possession of reports and deliverables does not give Client rights in or to SBS' methods of research, process of analysis or other intellectual property. In no event may such reports or deliverables be shared with third parties without SBS' prior written consent. SBS may retain copies and use them for review of any matter arising out of this Agreement, but SBS has no obligation to maintain any copies for longer than 7 years.

6. MISCELLANEOUS

6.1 This Agreement constitutes the entire understanding between SBS and Client with respect to the Services described in this Agreement and supersedes all prior oral and written communications. If there is a conflict between these Terms and the Proposal, these Terms will govern. Any Services Guide provided by SBS contains a general description of services and deliverables and is not a representation, warranty, or guaranty of any kind.

6.2 SBS is an Equal Opportunity Employer. SBS does not and will not discriminate in employment and personnel practices on the basis of race, sex, age, handicap, religion, national origin or any other basis prohibited by applicable law. Hiring, transferring and promotion practices are performed without regard to the above listed items.

6. 3 Client may not assign or transfer this Agreement without the prior written consent of SBS. The sale or transfer of a majority of the ownership interests (or right to direct the operations) of Client, or the sale or transfer of a substantial portion of its business assets or any similar transaction will be considered a prohibited assignment. If Client assigns this Agreement or undergoes a change of control without consent, SBS may elect to treat this Agreement as if Client cancelled

without cause subject to exercise of the rights provided Section 1.5.

6.4 This Agreement is binding upon the trustees, administrators, successors and assigns of the parties. This Agreement may not be modified orally or in any other manner except by a writing signed by the parties. This Agreement and any action regarding it will be governed by the law of South Dakota, without regard for conflicts of laws principles. Any action arising under this Agreement must be venued in the state or federal courts serving Lake County, South Dakota.

6.5 The provisions of Sections 1.5, 2.3, 4.3. 4.4, Section 5, and Section 6 will survive the expiration or termination of this Agreement for any reason.

6.6 Counterparts and Delivery. This Agreement may be executed in separate counterparts by the parties which taken together will constitute one document. A counterpart signature page delivered by facsimile, email or other means of electronic communication will be deemed to be an original for all purposes of this Agreement.