

Information Systems Specialist

Management Position (\$113,795.86 - \$132,320.77)

SYNERGY NORTH CORPORATION distributes electricity to approximately 50,000 residential customers and 6,000 commercial customers located in Thunder Bay and Kenora, Ontario. It is our mission to provide outstanding energy services in a safe, reliable, and trusted manner to our communities in order to power people's lives.

Reliable electricity depends on more than poles and wires. It also depends on the information systems that support every part of our utility. From maintaining the applications our employees rely on each day to protecting critical infrastructure from evolving cyber threats, our Information Systems team helps ensure our utility operates securely, efficiently, and reliably. We are seeking an experienced and collaborative Information Systems Specialist to join our team. In this role, you will administer and enhance our enterprise technology environment, lead infrastructure and cybersecurity initiatives, and support projects that strengthen our operations. If you enjoy solving complex technical challenges and want to make a meaningful contribution to the communities we serve, we encourage you to apply for this full time, permanent position based in Thunder Bay, Ontario.

As an Information Systems Specialist, you will:

- Administer and maintain enterprise server, storage, cloud, network, and identity management environments across corporate IT and operational technology networks.
- Support and secure confidential corporate applications, including payroll, human resources, finance, and executive reporting systems.
- Implement and maintain cybersecurity controls, governance practices, and regulatory compliance requirements.
- Monitor system performance, investigate and resolve complex technical issues, and serve as the primary escalation resource for critical incidents.
- Lead technology projects, including system upgrades, cloud initiatives, automation projects, cybersecurity improvements, and infrastructure enhancements.
- Design, test, and maintain disaster recovery and business continuity solutions.
- Conduct cybersecurity assessments, vulnerability reviews, security audits, and compliance reporting.
- Collaborate with internal stakeholders, vendors, consultants, and service providers to deliver technology solutions that improve business performance.
- Research emerging technologies and recommend innovative solutions that enhance security, reliability, and operational efficiency.
- Provide technical leadership, mentoring, and guidance to Information Systems team members while supporting emergency response and incident management activities.

What You'll Bring:

- A degree or diploma in Computer Science, Information Systems, or a related discipline, or an equivalent combination of education and experience.
- A minimum of five (5) years of progressively responsible experience supporting enterprise information systems and infrastructure.
- Demonstrated experience administering enterprise servers, cloud, network, and cybersecurity technologies.
- Experience leading technical projects and implementing technology solutions.
- Strong analytical, problem solving, organizational, and communication skills, with the ability to manage multiple priorities.
- A commitment to confidentiality, cybersecurity, regulatory compliance, and continuous improvement.
- Competency within the meaning of the Occupational Health and Safety Act.

Working Conditions & Employment Requirements

The successful candidate must be capable of responding to critical business and cybersecurity incidents outside of normal working hours, have and maintain a valid Ontario class G driver's license, successfully complete security screening and background checks.

Why Join Synergy North?

You will join a team committed to Safety, Reliability, Community, and Excellence. We offer a rewarding career with competitive compensation, comprehensive benefits, ongoing professional development, and the opportunity to apply your expertise to secure and enhance the technology that powers the communities we serve.

Our Commitment to Inclusion

Synergy North is committed to fostering an inclusive, respectful, and accessible workplace. We welcome applications from all qualified candidates and will provide accommodation throughout the recruitment process in accordance with applicable legislation. If you require accommodation at any stage, please let us know.

Applicants are asked to email a single PDF document containing their resume and cover letter to recruit@synergynorth.ca

Visit synergynorth.ca/careers for a complete position description.

Applications will be reviewed starting **August 14, 2026**, and will continue to be accepted until position is filled.

This position is currently vacant, artificial intelligence may be used to assist in the screening process; however, hiring decisions will be made based on an objective recruitment process fulfilled by a panel of subject matter experts.

POSITION DESCRIPTION

POSITION TITLE:	Information Systems Specialist
DIVISION:	Customer & Information Services
SUPERVISOR:	Information Systems Manager
AFFILIATION:	Management

Under the general direction of the Information Systems Manager, the Information Systems Specialist is responsible for the administration, security, governance, and continuous improvement of corporate information systems and technology services. The incumbent provides senior-level technical expertise, project leadership, cybersecurity oversight, and escalation support for critical business systems.

This position acts as a lead resource for complex technical initiatives, supports confidential corporate systems including human resources, payroll, and financial applications, and performs cybersecurity compliance, auditing, and risk management functions across the organization. The incumbent exercises a high degree of independent judgment in the administration of sensitive systems, evaluation of technology solutions, implementation of cybersecurity controls, and coordination of technology projects.

Duties & Responsibilities of the Information Systems Specialist include:

1. Information Systems Administration

- Administer and maintain corporate server, storage, cloud, and network infrastructure including IBM i, Windows, Linux, Microsoft 365, Azure, and related technologies on both the IT and OT networks.
- Administer confidential corporate applications and databases including payroll, human resources, financial, and executive reporting systems.
- Administer corporate identity, access management, authentication, and privileged account controls.
- Monitor, maintain, and optimize the availability, integrity, security, and performance of corporate systems and services by proactively identifying, troubleshooting, and resolving issues.
- Design, implement, test, and maintain disaster recovery and business continuity solutions.
- Coordinate hardware and software acquisition activities including evaluation, procurement recommendations, implementation, and lifecycle management.

2. Cyber Security Governance and Compliance

- Implement cybersecurity policies, standards, procedures, and technical controls in accordance with corporate requirements and industry standards.
- Conduct security audits, compliance reviews, access reviews, and vulnerability assessments across corporate systems and technology environments.
- Monitor cybersecurity events, investigate incidents, coordinate response activities, and recommend corrective actions.
- Perform security reviews of systems, projects, vendors, and technology changes.
- Audit compliance with cybersecurity controls and regulatory requirements and prepare reports for management.
- Coordinate remediation activities resulting from security assessments, audits, and incident investigations.
- Maintain cybersecurity documentation, risk registers, and audit evidence.
- Participate as a member of the Cyber Incident Response Team

3. Project Leadership and Continuous Improvement

- Lead technology projects from planning through implementation, including upgrades, migrations, automation initiatives, cybersecurity projects, and system enhancements.
- Coordinate project activities involving internal stakeholders, external vendors, consultants and service providers.
- Develop project plans, technical specifications, implementation strategies, and status reporting.
- Identify opportunities to improve operational efficiency, service delivery, system reliability, and customer experience through the better utilization of existing technologies.
- Research emerging technologies and make recommendations regarding adoption, implementation, and investment priorities.
- Facilitate automation and business process improvement initiatives throughout the organization.

4. Escalation Support and Technical Leadership

- a. Serve as the primary escalation point for complex technical incidents and service issues.
- b. Provide technical guidance, mentoring, and knowledge transfer to other Information Systems staff.
- c. Coordinate resolution of major incidents and communicate status updates to stakeholders and management.
- d. Develop and maintain technical standards and best practice documents.
- e. Provide technical leadership during emergency response, disaster recovery, and business continuity activities.

5. Confidential and Corporate Support Functions

- a. Administer and support systems containing confidential employee, payroll, financial, customer, and corporate information.
- b. Participate in investigations, audits, and reviews involving sensitive corporate data and systems.
- c. Manage access controls and segregation of duties for confidential business applications.
- d. Support compliance, governance, and risk management initiatives involving sensitive corporate information.
- e. Maintain confidentiality and security of all information accessed through assigned duties.

6. Vendor and Stakeholder Management

- a. Liaise with third-party vendors, consultants, auditors, and service providers regarding technology solutions, cybersecurity requirements, and service delivery.
- b. Participate in contract evaluations, technical reviews, and vendor performance assessments.
- c. Represent the Information Systems department on corporate initiatives, committees, and cross-functional projects.

7. Other Duties

- a. Participate in after-hours support, emergency response, and incident management as required.
- b. Perform such other related duties as may be assigned.

COMPETENCIES

- 1. Safety Leadership
- 2. Planning & Organizing
- 3. Problem Solving & Decision Making
- 4. Communication
- 5. Accountability
- 6. Quality & Attention to Detail
- 7. Continuous Improvement
- 8. Risk & Regulatory Compliance

MANDATORY QUALIFICATIONS & EXPERIENCE

- 1. Degree or diploma in Computer Science, Information Systems, or a related discipline, or an equivalent combination of education and experience.
- 2. Minimum five (5) years of progressively responsible experience supporting enterprise information systems and infrastructure.
- 3. Demonstrated experience administering enterprise server, network, cloud, and cybersecurity technologies.
- 4. Experience leading technical projects and coordinating work involving multiple stakeholders.
- 5. Strong understanding of cybersecurity principles, risk management, compliance, and security controls.
- 6. Demonstrated ability to exercise sound judgment and maintain confidentiality when handling sensitive corporate information.
- 7. Excellent analytical, organizational, problem-solving, and communication skills.
- 8. Ability to work independently with minimal supervision while managing competing priorities.
- 9. Must be competent within the meaning of the Occupational Health and Safety Act.

PREFERRED QUALIFICATIONS & EXPERIENCE

- 1. Professional certifications such as CISSP, CISM, Security+, CCNA, Azure Administrator, Microsoft Certified Professional, PMP, ITIL, or equivalent.
- 2. Experience administering payroll, human resources, financial, or enterprise resource planning systems.
- 3. Experience conducting cybersecurity assessments, vulnerability assessments, or compliance reviews.
- 4. Experience in utility, critical infrastructure, or operational technology environments.
- 5. Programming, scripting, automation, or systems integration experience.

CONDITIONS OF EMPLOYMENT

- 1. Must possess and maintain a valid Ontario Class G Driver's Licence.

2. Must successfully complete applicable security screening requirements (background check, etc), and periodic re-screenings
3. Must be available for after-hours support, incident response, and emergency situations as required.

DEPT APPROVAL:	K. SPEZIALE	HR APPROVAL:	A. KEMBEL
EFFECTIVE:	July 16, 2026	SUPERSEDES:	New