



Bastrop County Job Posting

804 Pecan Street, Bastrop TX 78602

(512) 581-7120

An Equal Opportunity Employer

Title: Cybersecurity Manager	Opening Date: September 4, 2025	Application Deadline: Open until filled	Job #: 250904
Department: Information Technology	Starting Salary: \$41.27 - \$43.27	Location: Bastrop, TX	Travel: Moderate

INTERNAL AND EXTERNAL JOB POSTING

This position can't be filled until October 1, 2025

Brief Job Description: The Cybersecurity Manager, will develop and oversee the implementation of our firm's cybersecurity strategies. Protecting our company's digital assets, ensure compliance with security standards, and mitigate risks is a crucial aspect of the position. The cybersecurity manager will also make sure our information assets and technologies are adequately protected from current and emerging threats.

Knowledge, Skills and Abilities: The ability to lead a team of cybersecurity professionals to ensure the security of company networks, systems, and data. Proficiency in security technologies and tools, including SIEM, firewalls, VPNs, data encryption protocols, and anti-malware solutions. Experience in cloud security and working with cloud platforms like AWS, Azure, or Google Cloud. Must have Extensive knowledge of regional and global cybersecurity frameworks, such as NIST, ISO 27001, SOC 2, CIS Controls, and Strong understanding of GDPR, CCPA, HIPAA, or similar data privacy regulations.

Minimum Qualifications: To perform this job successfully, an individual must be able to perform each essential duty satisfactorily, have a high school diploma or equivalent, and a valid Texas Driver's license (or a valid out of state Driver's license with the ability to obtain a TXDL within 90 days). The requirements listed below are representative of the knowledge, skill, and/or ability required. Reasonable accommodation may be made to enable individuals with disabilities to perform the essential functions.

Bastrop County does not discriminate on the basis of race, color, age, national origin, sex, religion or disability in employment or in its activities.

A Bastrop County Job Application is required and can be completed at:

[Bastrop County Employment Application](http://www.co.bastrop.tx.us/page/co.jobs)

Applications postmarked after the closing date will not be accepted. Unless otherwise indicated, regular attendance is an essential job requirement of all positions in the county. All positions requiring a degree and/or licensing require proof of degree and/or license. Your application for employment with Bastrop County may subject you to a criminal background check.

IMPORTANT NOTE TO ALL APPLICANTS: Only applicants scheduled for interviews will be contacted. If you are scheduled for an interview and require any reasonable accommodation in our interview process, please inform the hiring representative who calls you to schedule your interview. Whenever possible, please give the hiring representative sufficient time to consider and respond to your request. Thank you for considering employment with Bastrop County. This position has a six month eligibility list for qualified applicants. Visit our website at: <http://www.co.bastrop.tx.us/page/co.jobs>



BASTROP COUNTY, TEXAS

Job Description

Job Title: Cybersecurity Manager

Department: Information Technologies

FSLA Status: Exempt

Reports To: Information Technologies Director

SUMMARY: The Cybersecurity Manager, will develop and oversee the implementation of our firm's cybersecurity strategies. Protecting our company's digital assets, ensure compliance with security standards, and mitigate risks is a crucial aspect of the position. The cybersecurity manager will also make sure our information assets and technologies are adequately protected from current and emerging threats.

SUPERVISION RECEIVED AND EXERCISED:

Receives supervision from the Information Technologies Director;

Exercises supervision over Information Technologies lower-level employees;

ESSENTIAL DUTIES AND RESPONSIBILITIES include the following:

1. Develop, implement, and manage the organization's cybersecurity strategy and roadmap while leading a team of professionals to secure networks, systems, and data;
2. Monitor security systems, conduct risk assessments, perform vulnerability testing, penetration testing, and lead threat hunting to identify and mitigate potential cyber risks;
3. Oversee incident detection, investigation, and response processes, ensuring timely resolution of breaches and leading forensics and recovery efforts;
4. Ensure compliance with cybersecurity regulations (e.g., GDPR, HIPAA, ISO 27001), develop and enforce security policies, and maintain necessary documentation and procedures;
5. Design, implement, and manage security technologies (e.g., firewalls, IDS, antivirus, encryption), and ensure timely application of patches and system updates;
6. Work closely with IT, legal, and business units to embed security into operational processes and align efforts across departments;
7. Conduct security awareness training, monitor evolving threats, and stay up to date with advancements to foster a security-first culture and adapt defenses proactively;
8. Performs related work or duties as assigned by the Supervisor(s);

OTHER FUNCTIONS: Performs other job related duties as directed by supervisor(s). **Regular attendance is considered an essential function of this position.** **NOTE:** The essential functions describe the general nature and level of work being performed by employees holding this position. This is not intended to be a comprehensive listing of all duties and responsibilities required, nor is all duties listed necessarily performed by any one employee so classified.

MINIMUM QUALIFICATIONS: To perform this job successfully, an individual must be able to perform each essential duty satisfactorily, have a high school diploma or equivalent, and a valid Texas Driver's license. The requirements listed below are representative of the knowledge, skill, and/or ability required. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

Knowledge of:

Extensive knowledge of regional and global cybersecurity frameworks, such as NIST, ISO 27001, SOC 2, and CIS Controls;
Experience in data protection and cybersecurity, including incident management, security incident response frameworks, and disaster recovery planning;
Proficiency in security technologies and tools, including SIEM, firewalls, VPNs, data encryption protocols, and anti-malware solutions;
Experience in cloud security and working with cloud platforms like AWS, Azure, or Google Cloud;
Strong understanding of GDPR, CCPA, HIPAA, or similar data privacy regulations;
Hands-on experience with vulnerability assessments, penetration testing, and ethical hacking;
Strong leadership and team management skills, with experience leading cybersecurity initiatives;
Solid analytical and problem-solving skills, with the ability to identify and mitigate data security risks;
Excellent communication skills, with the ability to work cross-functionally with IT, legal, and business stakeholders;
Standard office policies, procedures, and equipment;
Bastrop County policies and procedures.

Ability to:

Read and understand technical manuals, procedural documentation, and OEM guides;
Recognize, analyze, and resolve network problems;
Provide training on technology equipment and software to users in user-friendly language and format;
Quickly identify and learn appropriate software and hardware;
Ability to maintain strong inter-personal skills;
Function independently, exercise good judgment, manage multiple projects, and meet deadlines;
Demonstrate initiative and professionalism;
Adjust to frequently changing priorities;
Record and disseminate accurate information from telephone conversations and personal contact;
Be detail oriented, and have strong communication, interpersonal, problem solving, analytical, organizational, conflict resolution, and stress tolerance skills;
Communicate clearly and concisely, both verbally and in writing;
Understand and follow verbal and written instructions;
Properly interpret, understand and make decisions in accordance with laws, regulations and policies;
Perform multiple tasks simultaneously in a timely manner;
Communicate clearly and concisely, both verbally and in writing;
Conduct business with the public and employees in a professional and courteous manner;
Establish and maintain effective working relationships with those contacted in the course of the job;
Operate equipment required to perform essential job functions;
Work independently in the absence of supervision;
Work in a safety-conscious environment and to follow and promote good safety practices;
Handle exposure to potentially hostile individuals;
Maintain confidentiality of information encountered in work activities at all times.

Physical Demands:

The physical demands described here are representative of those that must be met by an employee to successfully perform the essential duties of this job. Reasonable accommodations may be made to enable individuals with disabilities to perform the essential functions.

Maintain effective audio-visual discrimination and perception needed for:

Making observations, reading and writing, operating assigned equipment, and communicating with others; Employee must have visual abilities including close vision, distance vision, depth perception, peripheral vision, and the ability to adjust focus.

Maintain physical condition needed to accomplish the performance of assigned duties and responsibilities, which may include:

Walking, sitting, or standing for long periods of time; Lifting and carrying materials weighing up to 25 pounds such as files or stacks of records; Occasional climbing, stooping, crawling, squatting, &/or kneeling.

Maintain mental capacity sufficient to accomplish the performance of assigned duties and Responsibilities, which may include:

Handling stressful situations;
Interpreting federal laws and regulations;
Effective interaction and communication with others;
Prepare clear and concise reports;
Making sound decisions in a manner consistent with the essential job functions.

EXPERIENCE, EDUCATION, and LICENSING:

Any combination of experience and training that would likely provide the required knowledge and abilities is qualifying. A typical way to obtain the knowledge and abilities would be:

Experience:

Demonstrable experience as a Cybersecurity Manager, Information Security Officer, or similar role with at least 5 years in cybersecurity management;

Experience in data protection and cybersecurity, including incident management, security incident response frameworks, and disaster recovery planning;

Education:

Master's degree in information security, Cybersecurity, or related fields.

Bachelor's degree in computer science, Information Security, or similar role with at least 5 years in cybersecurity management, and/or training with major course work in computer science, management information systems, voice or data management experience or a related field is preferred;

High School diploma or equivalent.

Licensing:

SELECTION GUIDELINES:

Formal application; rating of education and experience; oral interview; reference and other background

checks; job-related tests may be required.

***** This position is subject to random and/or reasonable suspicion and/or post-accident testing for drugs and alcohol.*****

This job description does not constitute an employment agreement between the employer and employee and is subject to change by the employer as the needs of the employer and requirements of the job change. The employee further understands, and accepts, that this position falls under the provision of an "At Will" employment, and under no circumstances is a contract for employment.