BINGHAM COUNTY

Is Recruiting for the Position of

Cybersecurity Technician
September 8th 2026

Salary: Effective October 1st 2026 Starts at $27.54-$30.97/ hour – DOQ/DOE
Full time - County Benefits Included:
Including 13 Paid Holidays/6 Weeks Paid Parental Leave, Health Insurance, Public Employee Retirement System of Idaho (PERSI)
Closing Date: Open Until Filled

Pay Grade: N26 FLSA Designation: Non-Exempt

Purpose Of Class/Primary Function

Under direction of the Information Technology Director, Systems and Network Administrator, or designee, the Cybersecurity Technician is responsible for supporting, monitoring, maintaining, and improving Bingham County cybersecurity systems, procedures, and safeguards. The position assists in protecting County computer systems, networks, servers, cloud services, endpoints, law enforcement systems, user accounts, applications, and data from unauthorized access, misuse, disruption, or loss.

The Cybersecurity Technician performs security monitoring, investigates suspicious activity, assists with incident response, supports vulnerability management, reviews logs and alerts, documents findings, and helps implement cybersecurity controls. The position also assists the System Support Specialist and other Information Technology staff with support duties as needed, including desktop support, server and workstation support, software deployment, user support, hardware troubleshooting, and general technology service requests.

The position works with County departments, outside vendors, state agencies, law enforcement technology partners, and other Information Technology staff to maintain secure and reliable technology operations. Reasonable accommodations will be considered for qualified individuals with disabilities to perform the essential functions of this role.

Essential Duties and Responsibilities (will vary by assignment)

- Monitor County networks, servers, endpoints, firewalls, cloud services, email systems, remote access systems, security tools, and other technology platforms for suspicious activity, vulnerabilities, and security events.

- Review and analyze security alerts from endpoint protection, firewall systems, email security platforms, vulnerability scanners, Microsoft 365 / Entra ID tools, logging systems, and other cybersecurity systems.
- Investigate phishing reports, malware alerts, suspicious logins, account compromise indicators, unauthorized access attempts, data loss concerns, and other potential cybersecurity incidents.
- Support with cybersecurity incident response, including documentation, triage, containment support, evidence preservation, communication, recovery coordination, and after-action review.
- Analyze and isolate cybersecurity issues affecting desktops, servers, networks, cloud services, user accounts, applications, law enforcement systems, and physical security systems.
- Support vulnerability management by assisting with vulnerability scans, reviewing findings, prioritizing risks, tracking remediation, validating fixes, and preparing reports.
- Facilitate with patch management review and security update tracking for servers, workstations, applications, network devices, and other County technology systems.
- Monitor user authentication activity, privileged access, remote access, multi-factor authentication, conditional access, and directory service activity for security concerns.
- Aid with configuration and review of authentication and authorization of directory services, including Active Directory, Microsoft Entra ID, group membership, role assignments, and access permissions.
- Support Microsoft Entra ID, Intune, Office 365, Microsoft security tools, endpoint protection, email security, remote access controls, and other identity or cloud security systems.
- Assist with firewall, VPN, intrusion detection, endpoint protection, security logging, vulnerability scanning, and other cybersecurity-related systems.
- Aid with securing LANs, WANs, network segments, Internet and Intranet systems, server infrastructure, wireless networks, and remote access systems.
- Assist System Support Specialist staff as needed with maintaining, installing, and supporting server and desktop systems, analyzing and isolating PC, server, network, software, hardware, and storage issues, and responding to user support requests.
- Aid with software deployment, workstation setup, security updates, printer and scanner support, mobile device support, user account support, and other general Information Technology support tasks as assigned.
- Support and assist with cybersecurity support for 24x7 law enforcement systems and networks, including coordination with state agencies, corporate vendors, dispatch, jail, patrol, courts, and other public safety technology partners.
- Assist with cybersecurity support for physical security systems, including IP cameras, DVRs, access control, patrol fleet connectivity, and other network-connected security systems.
- Assist with cybersecurity review of new hardware, software, cloud services, vendor services, network changes, and technology projects.
- Maintain cybersecurity documentation, including incident notes, system diagrams, procedures, asset information, security configurations, risk findings, remediation status, and user guidance.
- Prepare security reports, incident summaries, vulnerability summaries, audit support materials, and recommendations for review by IT leadership.

- Expedite and assist with implementation and maintenance of cybersecurity policies, procedures, standards, controls, and best practices.
- Train and assist County users by providing cybersecurity awareness, phishing prevention guidance, password and authentication guidance, data handling guidance, and general security support.
- Help promote a security-aware culture by communicating risks and practical security practices to employees in a clear and professional manner.
- Protect confidentiality of County, law enforcement, jail, court, employee, financial, operational, and public information.
- Ensure continuity and statutory compliance through adequate backup awareness, cybersecurity protocols, incident documentation, and security practices.
- Update job knowledge by participating in educational opportunities, reading professional publications, maintaining professional networks, and participating in professional organizations.
- Work with outside vendors, consultants, state agencies, and other governmental entities on cybersecurity-related matters.
- Perform other related duties as assigned.

Specialty Areas

- **Required**: Experience or working knowledge of cybersecurity practices related to Windows Active Directory, Microsoft infrastructure services, endpoint protection, firewalls, cloud services, remote access, vulnerability management, user authentication, and network security. Must be able to understand, support, and help secure 24x7 law enforcement systems and networks. Must be able to work with various state agencies and corporate vendors to troubleshoot state and local interagency law enforcement networks and systems. Must be able to learn and become proficient in various specialty government software suites and physical security systems, including IP cameras, DVRs, patrol connectivity, and physical access control. Must be available for on-call status. Will support various additional specialty areas as assigned. Must be able to adapt and learn.
- **Preferred**: Experience with Microsoft Entra ID, Intune, Office 365, Microsoft Defender or equivalent endpoint protection, Group Policy, Microsoft infrastructure services, Dynamic Host Configuration Protocol, Domain Name Systems, remote authentication, VMware server virtualization, VOIP telephony systems, firewall administration, vulnerability scanning, phishing prevention, SIEM or log management tools, incident response, security awareness training, and day-to-day network or security troubleshooting.

Qualifications and Competency Requirements

Essential:

- Knowledge of cybersecurity principles, including confidentiality, integrity, availability, least privilege, defense in depth, access control, endpoint security, network security, vulnerability management, and incident response.
- Knowledge of common cybersecurity threats, including phishing, malware, ransomware, credential theft, unauthorized access, data exposure, social engineering, and misuse of privileged access.

- Knowledge of Microsoft Office 2019 and above, Microsoft Exchange or Office 365, Microsoft Server 2019 and above, Active Directory, Microsoft Entra ID, Intune, VMware, Hyper-V, SAN and NAS storage devices, firewalls, Remote Desktop Protocol, Remote Apps, Internet Protocol networking and management, server hardware, workstations, IP printers, scanners, mobile devices, and all-in-one workstations.
- Network, software, hardware, cloud service, and storage troubleshooting skills.
- Review logs, alerts, vulnerability results, user reports, and system activity to identify potential cybersecurity issues.

Ability to:

- Assist with incident response, including documenting facts, preserving information, escalating concerns, and supporting recovery activities.
  document findings, incidents, remediation steps, procedures, and recommendations.
- Communicate cybersecurity concerns clearly to technical and non-technical users.
- Maintain confidentiality and exercise sound judgment when handling sensitive information.
- Perform wireless network troubleshooting, deployment, and management awareness.
- Assist with System Support Specialist duties and general Information Technology support tasks when needed.
- Self-start and stay motivated.
- Multi-task and work on various projects simultaneously.
- Work with outside vendors and consultants on a regular basis.
- Interface with all departments and personnel.
- Interface and communicate with third-party vendors.
- Communicate effectively through oral and written means.

Preferred:

- Two or more years of experience working in cybersecurity, information technology, systems administration, network administration, or related technical support.
- Experience working with law enforcement, PSAP, public safety, jail, courts, county government, or other government technology systems.
- Experience with Computer Arts County software suite and law enforcement software suite.
- Experience with Motorola CAD, E911, PSAP software, Idaho Supreme Court software and hardware, ArcGIS, or other government software systems.
- Experience with vulnerability scanning, cybersecurity incident response, security awareness training, phishing investigations, Microsoft security tools, Sophos firewalls or similar products, SIEM or log management tools, and endpoint detection and response systems.
- Relevant certifications such as CompTIA Security+, Network+, CySA+, Microsoft security certification, GIAC, SSCP, or equivalent training.

Work Environment:

- Works indoors in limited office space, with adequate lighting, temperatures, and ventilation. Limited outdoor work.
- Normal exposure to noise, stress, and frequent interruptions.
- Normal exposure to dirt and dust.
- Travels occasionally when needed to go to outlying offices, including Road & Bridge, Central Transfer Station, County Landfills, Extension Office, and other County locations.
- Incumbent will occasionally need to work in the County jail and law enforcement areas.
- May be required to work evenings, weekends, holidays, or off hours during cybersecurity incidents, outages, maintenance windows, emergency situations, critical security events, or urgent support needs.

Machines Typically Operated

- General computing, cybersecurity, and networking equipment, including phones, computers, servers, switches, routers, firewalls, fax machines, printers, scanners, mobile devices, physical security equipment, video systems, access control systems, and related County technology systems.

Essential Physical Abilities

- Sufficient clarity of speech and hearing, with or without reasonable accommodation, which permits the employee to discern verbal instructions and communicate effectively with the public and other employees in person and by telephone.
- Sufficient visual acuity, with or without reasonable accommodation, which permits the employee to comprehend written work instructions, review, prepare, and evaluate documents, review system information, and organize and file documents and materials.
- Sufficient manual dexterity, with or without reasonable accommodation, which permits the employee to operate a personal computer, standard office equipment, specialized technical equipment, and a motor vehicle.
- Sufficient strength to lift and carry objects up to 25 pounds occasionally.
- Sufficient personal mobility, flexibility, strength, and agility, with or without reasonable accommodation, which permits the employee to lift up to 25 pounds, sit and work at a keyboard for an extended period of time, and work in an office, jail, law enforcement, and County facility environment.
- Jobs in this class require, with or without reasonable accommodation, lifting or moving up to 25 pounds occasionally. The employee is regularly required to stand, walk, sit, bend, stoop, crouch, and stretch. The employee is frequently required to use hands to operate a computer keyboard and standard office equipment, to handle or feel, and to reach with hands and arms.

Licensing and Certification

- Possess a valid Idaho Class D driver's license.
- Must successfully pass required background checks.

- Cybersecurity or information technology certifications are preferred and may be required depending on assignment.
- Must maintain any required access, training, or certification necessary to support law enforcement, jail, court, County, or state-connected systems.

This class description lists the major duties and requirements of the position and is not all-inclusive. Incumbents may be expected to perform job-related duties not included in this document and may be required to have specific job-related knowledge and skills.

Benefits

Bingham County offers a highly competitive benefits package including membership in the Public Employee Retirement System of Idaho (PERSI), paid time off, holiday pay, paid parental leave, as well as medical, dental, vision and life insurance. If you would like to view all of the benefits Bingham County offers our full-time employees, please visit our website: www.binghamid.gov , then click on Human Resources and that will take you to our web page and on the left side you will see "Employee Benefits", if you click on this you will see our Benefits page.

How to Apply

A job description and the ***Application*** may be picked up at the Bingham County Courthouse, Department of Human Resources, Room 223 or you may find the application on our website: www.binghamid.gov. When you have completed the ***Application*** and have attached all of the required documentation, you may submit it by bringing it to the address listed above, or you may mail it to this address: 501 N Maple #202, Blackfoot, Idaho 83221. If you choose to mail it, it must be received in the office by 4.00pm on closing day, if there is one. You may also fax the paperwork to (208) 782-2681 or email it to L.Pope: lpope@binghamid.gov by the closing date and time.

The back page of the ***Application*** is an Authorization for Release of Records and Personal Information. You will need to sign this document in front of a Notary Public. You may bring a picture ID with you to the Courthouse and Laraine Pope in HR will notarize this page for you.

Items that must be attached to the Application

Valid Idaho Driver's License
Resume

If your application is not complete or does not have the required documentation, you may not be considered for this job posting.