SAN JOAQUIN COUNTY
Greatness grows here.

**Information Systems Division**

**Tristian Cormier, Director**
**Rod Baker**, *Assistant Director*
**Ken Hoach**, *SJGH CIO*
**Amanpreet Kaur,** *CISO*

Greetings,

The San Joaquin County Information Systems Security team is proud to present the San Joaquin County Cybersecurity Strategy and Roadmap. This Strategy represents the County's ongoing commitment to strengthening cybersecurity, protecting public services, and supporting the dedicated cybersecurity and IT practitioners across all County departments and partner agencies.

Representatives from County departments, and critical infrastructure partners collaborated in the development of this plan. Their shared insights helped shape a set of actionable goals and measurable objectives that will ensure effective and sustainable implementation across all areas of County government.

The priorities outlined in this Strategy focus on:

- Enhancing resilience through County-wide cyber governance
- Leveraging shared services and scalable technologies
- Standardizing security operations
- Improving Internet of Things (IoT) and Operational Technology (OT) Devices security protection
- Expanding workforce readiness and cybersecurity awareness
- Strengthening third-party and supply chain risk oversight

Through these coordinated efforts, San Joaquin County will improve its cybersecurity posture, maximize available State and Federal resources, and ensure a foundation of security that keeps pace with evolving cyber threats.

We are committed to achieving the goals established in this Strategy and positioning San Joaquin County as a leader in cyber resilience—one that protects sensitive data, ensures continuous delivery of critical public services, and maintains the trust of our residents.

Amanpreet Kaur, CISO, San Joaquin County

## EXECUTIVE SUMMARY

San Joaquin County Information Systems Division (ISD) and the Chief Information Security Office (CISO) are committed to identifying, mitigating and managing cybersecurity risks to protect consumer data and privacy. This journey is even more important in the face of ever-increasing threats, including advanced malware, Advanced Persistent Threats (APTs), well-funded and organized adversaries, and increasingly automated cybersecurity attacks.

The San Joaquin County Information Systems Division (ISD) Cybersecurity Strategic Roadmap (FY2026–FY2029) outlines a three-year plan to strengthen cyber resilience, protect sensitive data, and ensure the secure delivery of public services. Aligned with the Cybersecurity and Infrastructure Security Agency (CISA) strategic framework — Address, Harden, and Drive — this roadmap provides a clear pathway for maturing cybersecurity capabilities while supporting innovation, compliance, and operational continuity. Furthermore, Strategy is built around five pillars: Governance, Protection, Detection, Response, and Recovery.

This strategy establishes a **5-Pillar Cybersecurity Model** to:

- Strengthening governance and risk management
- Protect critical systems and data
- Detect and respond to incidents efficiently
- Build workforce awareness and cybersecurity culture
- Collaborate and ensure resilience across departments and partners

## MISSION STATEMENT

The Information Systems Division is dedicated to delivering secure, reliable, and innovative technology solutions that empower San Joaquin County departments to serve the public effectively. Our mission is to lead the County's cybersecurity strategy through centralized governance, resilient infrastructure, and proactive risk management—ensuring the confidentiality, integrity, and availability of critical systems and data while fostering a culture of security and continuous improvement.

## VISION STATEMENT

San Joaquin County will be a model of cybersecurity resilience, where trusted, secure, and innovative technology supports safe citizen services, protects critical infrastructure, and enables a proactive, risk-aware culture across all County operations

## GUIDING PRINCIPLES

- Security as a public service — protecting residents and community trust.
- Centralized governance and distributed execution — one framework, Countywide adoption.
- Risk based prioritization — focusing resources where they reduce the most risk.
- Transparency and accountability — clear ownership and communication.
- Continuous improvement — adapting to evolving threats and technologies.
- Resilience over perfection — emphasizing readiness and rapid recovery.

Cybersecurity Strategic Goals: 5-Pillar Framework

# Pillar 1 – Governance, Asset & Risk Management

## Objective:

Establish strong leadership, clear accountability, and consistent Countywide risk processes.

## Key components

- Centralized governance and policies
- Countywide risk register
- Vendor and third-party risk management
- Compliance with major data security and compliance frameworks designed to protect sensitive information, including but not limited to HIPAA, CJIS, IRS 1075, NIST CSF 2.0 where applicable

# Pillar 2 – Protection & Hardening

## Objective

Safeguard county assets, infrastructure, and sensitive information from compromise.

## Key components

- Zero Trust foundations
- System hardening and configuration management
- IoT and medical device security where applicable
- Data protection (encryptions, DLP, classification)
- Identity lifecycle and privileged access management
- Modernized vulnerability management

.

# Pillar 3 – Detection, Monitoring & Threat Response

## Objective:

Detect threats early, respond effectively, and minimize operational impact

## Key components

- Enhanced SIEM/SOC capabilities
- Updated incident response plans and playbooks
- Automated workflows and threat hunting
- Countywide incident reporting and escalation

# Pillar 4 – Workforce, Culture & Awareness

## Objective

Empower County employees and leaders to recognize threats and adopt secure behaviors.

## Key components

- Countywide cybersecurity training
- Phishing simulations
- Awareness campaigns and executive briefings
- Role-based training for high-risk departments

# Pillar 5 – Collaboration & Strategic Resilience

## Objective

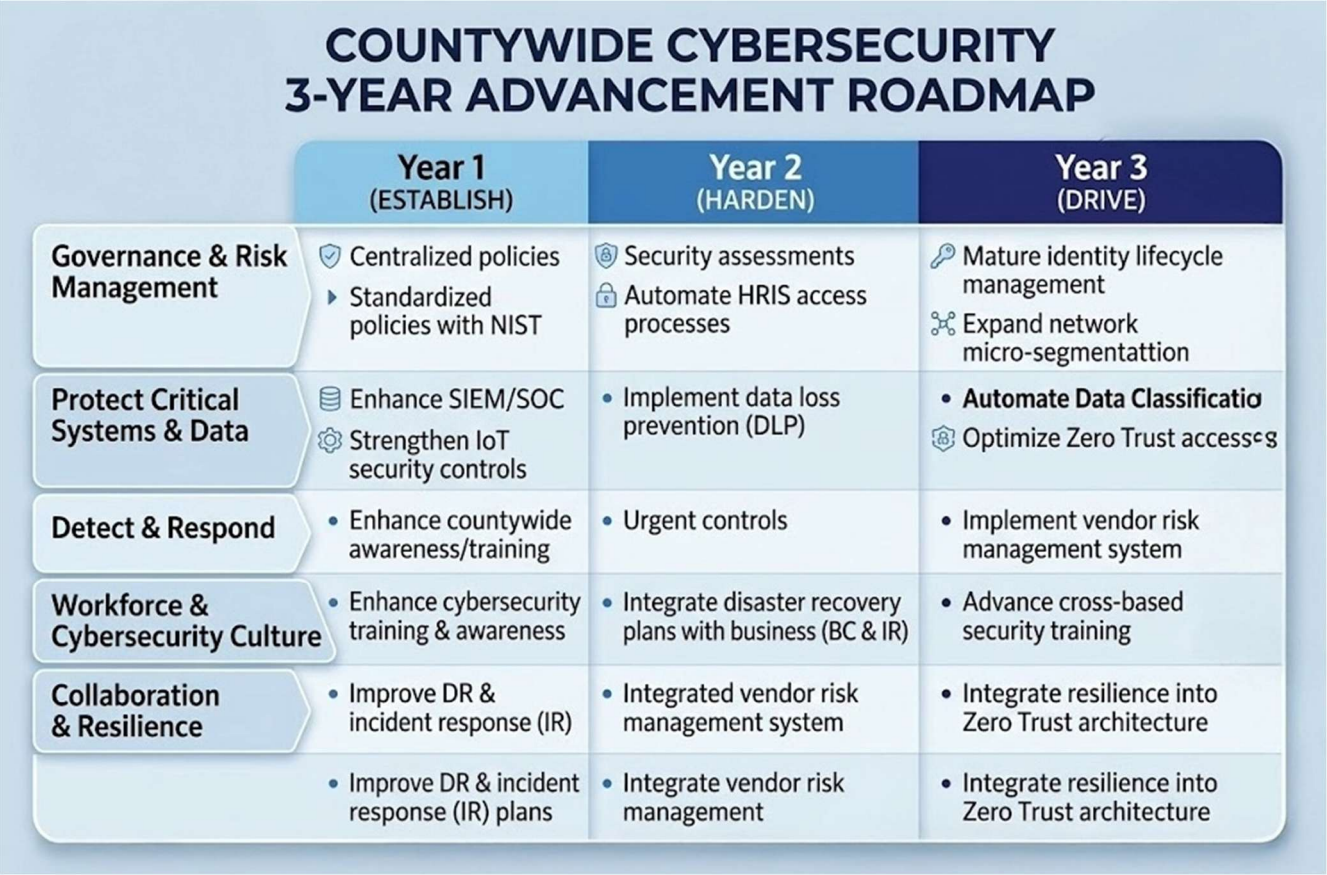
Strengthen resilience through coordinated planning, shared defenses, and collective preparedness.

## Key components

- Business continuity & disaster recovery improvements
- Countywide tabletop exercises
- Partnerships with local/state/federal agencies
- Shared intelligence and cross-department coordination

## 3-Year STRATEGIC ROADMAP

The roadmap follows a phased progression designed to build upon foundational improvements and evolve toward advanced resilience and integration:




# Address (Year 1 – Foundational Improvements):

## Objective:

Build a strong Countywide cybersecurity foundation. Formalize governance. Standardize security practices. Implement critical controls to reduce risk, improve visibility, and strengthen resilience across the County's digital environment.

- Establish a centralized cybersecurity governance framework for consistent oversight and accountability
- Enhance SIEM and SOC capabilities to improve threat detection and incident response
- Strengthen IoT security controls, including segmentation and asset visibility
- Formalize and Improve Third-Party Risk Management (TPRM) program
- Establish a Zero Trust access framework for identity and network security
- Enhance Countywide Cybersecurity training and awareness

# Harden (Year 2 – Maturity and Defense-in-Depth):

## Objective:

Advance security maturity across the enterprise. Strengthen monitoring, data protection, and resilience. Improve defenses against evolving threats through enhanced risk management, independent assessments, and stronger incident response capabilities.

- Conduct an independent security assessment and penetration testing
- Improve Disaster Recovery (DR), Business Continuity (BC), and Incident Response (IR) plans
- Conduct a cybersecurity tabletop exercise
- Strengthen secrets management and implement Data Loss Prevention (DLP) controls
- Launch a phased data classification program

# Drive (Year 3 – Optimization and Innovation):

## Objective:

Optimize and innovate cybersecurity operations. Automate processes, refine identity and access management, and expand Zero Trust principles. Focus on sustainability, agility, and advanced analytics to maintain a resilient security posture.

- Enhance Zero Trust Architecture across the County
- Expand network micro-segmentation
- Mature security metrics and visualization
- Refine identity lifecycle management processes
- Automate access provisioning and deprovisioning through the Human Resource Information System (HRIS)
- Automate incident response workflows

---

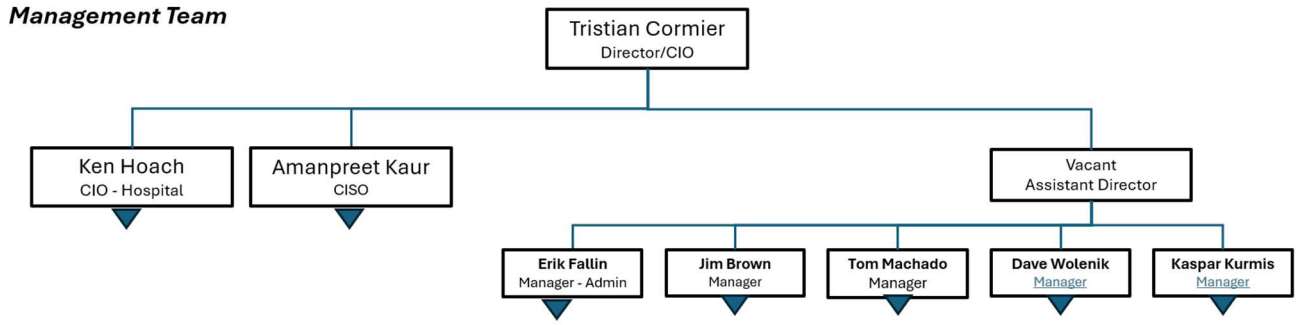
# What Residents Can Expect

- Better protection of personal information
- More reliable and secure public services
- Faster response to cyber incidents
- Increased transparency and accountability
- A stronger, more resilient County government

# Our Goal

San Joaquin County aims to be a leader in cybersecurity resilience—protecting the community, supporting public trust, and ensuring that essential services remain safe, secure, and available.

# ISD Organization Chart




## APPENDIX A ROLES AND RESPONSIBILITIES

**Board of Supervisors / County Executive (Director/CIO and CAO)**

- Approving cybersecurity strategy
- Allocate resources
- Require periodic reporting and accountability

**Chief Information Officer (CIO)**

- Lead overall technology vision and digital transformation
- Manage IT budget, portfolio, and governance policies
- Ensures alignment of cybersecurity with county objectives
- Collaborates with CISO on prioritization and resource allocation

**Chief Information Security Officer (CISO)**

- Lead county-wide cybersecurity strategy, governance, and compliance
- Chair Cybersecurity DISO Program
- Oversee risk management, security operations, and data protection
- Ensure alignment with HIPAA, CJIS, IRS-Pub 1075, NIST CSF, CIS Controls, and state mandates
- Reports posture and risks to CIO, Executive Leadership, and Board

**IT Directors / Department Heads**

- Ensure department compliance
- Identify departmental assets and risks
- Support training and incident reporting

**Security Operations (SOC) /Cybersecurity Team/ DISO's**

- Continuous monitoring
- Incident detection and response
- Vulnerability management
- Security Awareness Training
- Audit Response
- Data Classification
- Patch Management
- Confidential Data Flow Documentation

**All Employees**

- Complete annual training
- Report on suspicious activity
- Follow policies and secure behavior practices

**Vendors & Third Parties**

- Must comply with county security requirements
- Participate in security assessments as required
    - Report security incidents in a timely manner

---

## Technical Glossary

- **Asset:** An item of value to stakeholders. An asset may be tangible (e.g., a physical item such as hardware, firmware, computing platform, network device, or another technology component) or intangible (e.g., humans, data, information, software, software, software, capability, function, service, trademark, patent, intellectual property, image, or reputation).
- **Advanced Persistent Threat (APT):** A sophisticated and long-term cyberattack conducted by organized, well-funded adversaries who infiltrate a network and remain undetected to steal information or disrupt operations.
- **Artificial Intelligence (AI) Monitoring**: The use of machine learning and analytics to detect anomalies, cyber threats, and suspicious behavior in real time.
- **Asset Management:** The process of maintaining a complete and current inventory of technology hardware, software, and data to ensure proper security controls are applied.
- **Business Continuity (BC):** Planning and preparation to ensure essential services continue during and after a disruption such as a cyberattack or natural disaster.
- **Cybersecurity:** Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation
- **Cybersecurity & Infrastructure Security Agency (CISA):** The U.S. federal authority that provides cybersecurity guidance, threat intelligence, and resilience frameworks for critical infrastructure.
- **Data Classification:** Organizing data based on sensitivity (e.g., Public, Internal, Confidential, Restricted) to ensure proper handling and protection.
- **Data Loss Prevention (DLP):** Technology and processes used to prevent unauthorized access, use, sharing, or transfer of sensitive data.
- **Disaster Recovery (DR):** The capability to restore systems, data, and operations after a major outage or cyber incident.
- **Governance:** Executive-level direction and decision-making that ensures cybersecurity practices align with laws, policies, and risk reduction goals.
- **Incident Response (IR):** A coordinated approach to detecting, investigating, containing, and recovering from cybersecurity incidents.
- **Information Systems Division (ISD):** The County's centralized IT organization responsible for technology services, security, and systems support.
- **Internet of Things (IoT):** Network-connected devices such as cameras, sensors, or smart building systems that require security controls due to increased risk exposure.
- **Multifactor authentication:** An authentication system that requires more than one distinct authentication factor for successful authentication. Multifactor authentication can be performed using a multifactor authenticator or by a combination of authenticators that provide different factors. The three authentication factors are something you know, something you have, and something you are.
- **Micro-Segmentation**: Dividing networks and systems into secure zones to prevent threat actors from moving laterally after gaining access.
- **NIST Cybersecurity Framework (NIST CSF):** A nationally recognized standard for managing cybersecurity risk, built around functions: Identify, Protect, Detect, Respond, and Recover.

- **Operational Technology (OT) devices** are systems and equipment that monitor or control physical devices, processes, and events within industrial, infrastructure, or facility environments
- **Personally Identifiable Information (PII):** Any data that can identify an individual (e.g., name, SSN, address).
- **Protected Health Information (PHI):** Health-related information protected under HIPAA privacy and security regulations.
- **Privileged Access Management (PAM):** Controls that restrict and monitor elevated system access for accounts that can make security-impacting changes.
- **Risk:** A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.
- **Risk Register:** A documented list of security risks, including their likelihood, impact, and mitigation strategy.
- **Security Information and Event Management (SIEM):** A system that collects and analyzes logs from multiple sources to detect and alert cybersecurity threats.
- **Security Operations Center (SOC):** A team and facility responsible for continuous monitoring and response to cyber threats.
- **Secrets Management:** Tools and processes that securely store passwords, API keys, encryption keys, and other sensitive authentication credentials.
- **Threat:** Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service
- **Vendor / Third-Party Risk Management:** Evaluation of external partners to ensure they meet security requirements and do not introduce risk to the County.
- **Zero Trust Architecture:** A modern security model that assumes no user or system is trusted by default—access is continuously verified and limited to what is necessary